SuSE Linux Enterprise Server 8

per IBM iSeries e IBM pSeries

Amministrazione

Edizione 2004

Copyright ©

Il presente prodotto è proprietà intellettuale della SuSE Linux AG.

È lecito copiare questo manuale interamente o parzialmente, a condizione che, su ogni copia, venga riportata anche la presente nota riguardante i diritti d'autore.

Nonostante tutte le informazioni contenute in questo manuale siano state raccolte con estrema accuratezza, non è tuttavia possible escludere del tutto la presenza di indicazioni non corrette. La SuSE Linux AG, gli autori ed i traduttori non si assumono alcuna responsabilità giuridica e non rispondono di eventuali errori ovvero delle rispettive conseguenze.

Molte delle denominazioni dei componenti di software ed hardware adottati in questo materiale sono anche marchi depositati e vengono riportate senza che ne sia garantito il libero usufrutto. La SuSE Linux AG si orienta fondamentalmente alla dicitura usata dai produttori.

La riproduzione di nomi di prodotti o nomi commerciali etc. (anche privi di contrassegno specifico) nel presente manuale non significa che sussista la facoltà di usufruire liberamente di tali denominazioni (ai sensi della legislazione vigente in materia di marchi di fabbrica e di protezione dei marchi di fabbrica).

Le designazioni seguenti sono marchi registrati della International Business Machines Corporation negli Stati Uniti, e/o altri paesi: IBM, AS/400, AIX, OS/400, iSeries, pSeries, Redbook, DB2, and PowerPC.

Vi preghiamo di rivolgere eventuali comunicazioni e commenti all'indirizzo sottostante: documentation@suse.de

autori:	Frank Bodammer, Stefan Dirsch, Roman Drahtmüller, Karl Eichwalder, Werner Fink, Dennis Geider, Carsten Groß, Olaf Hering, Andreas Jaeger, Jana Jaeger, Klaus Kämpf, Olaf Kirch, Hubert Mantel, Michael Matz, Johannes Meixner, Lars Müller, Anas Nashif, Susanne Oberhauser, Edith Parzefall, Peter Poeml, Marc Rührschneck, Marcus Schaefer, Klaus Singvogel, Andreas Schwab, Martin Sommer, Klaus G. Wagner, Christian Zoz
traduttori:	Barbara Improta Mann, Gaetano Lazzara
redazione:	Antje Faber, Dennis Geider, Roland Haidl, Jana Jaeger, Edith Parzefall, Peter Reinhart, Marc Rührschneck, Thomas Schraitle, Martin Sommer, Rebecca Walter
formato:	Manuela Piotrowski, Thomas Schraitle
composizione:	LaTeX

Questo manuale è stato stampato su carta sbiancata senza cloro.

Introduzione

Presentazione

Questo manuale vi aiuterà ad amministrare il vostro SuSE Linux Enterprise Server sistemi iSeries e pSeries della IBM. Verrà descritto quanto necessario per configurare il sistema e verranno fornite alcune nozioni fondamentali sul networking.

YaST2, il tool di amministrazione principale di SuSE Linux Enterprise Server, vi mette a disposizione una serie completa di moduli che vi consentiranno di amministrare il vostro sistema centralmente. Questo manuale tratterà i moduli di YaST2 necessari per configurare e controllare il sistema.

Inoltre verrà descritto come configurare hardware aggiuntivo. p.e. stampanti.

Infine verrà trattata la configurazione della rete e diversi servizi di rete importanti con informazioni utili sulla sicurezza della rete e l'integrazione di SuSE Linux Enterprise Server in reti eterogenee.

A chi si rivolge questo manuale

Questo manuale è stato concepito per un pubblico che conosce:

- la terminologia di OS/400 e del firmware dei pSeries.
- l'ambiente hardware del sistema iSeries o pSeries e nella fattispecie dell'ambiente di rete.
- le nozioni basilari per l'impiego di Linux o Unix.

Convenzioni tipografiche

Nel presente manuale vengono applicate le seguenti convenzioni tipografiche:

Contrassegno	Significato
YaST	indicare il nome del programma
`/etc/passwd`	indicare il file o una directory
⟨*platzhalter*⟩	la sequenza di caratteri `platzhalter` (incl. parentesi graffa) è da sostituire con il valore effettivo
`PATH`	una variabile dell'ambiente con il nome `PATH`
`192.168.1.2`	il valore di una variabile
`ls`	l'indicazione di un comando da immettere
`user`	l'indicazione di un utente
`terra:~ # ls`	immissione di `ls` nella shell dell'utente `root` nella directory home sul computer "terra"
`tux@terra:~ > ls`	immissione di `ls` nella shell dell'utente `tux` (nome ufficiale del Pinguino Linux) nella directory home sul computer computer "terra"
`C:\> fdisk`	prompt di DOS con immissione di comando `fdisk`
Alt	un tasto da premere; tasti da premere l'uno dopo l'altro sono separati da uno spazio
Ctrl + Alt + Canc	tasti da premere contemporaneamente hanno un `'+'`
"Permission denied"	avviso del sistema
'Aggiornare il sistema'	voci di menu, bottoni
"Modo DMA"	convenzioni, definizioni di nomi, cosiddetto…

Norimberga, 26 gennaio 2004

Il vostro SuSE team

Indice

Introduzione iii

I Configuration **1**

1 YaST2 nel modo testo (ncurses) **3**

L'uso 3

Usare i moduli 5

Richiamare singoli moduli 5

YOU: YaST Online Update 6

2 YaST2 nel modo grafico **9**

Inizializzare YaST2 10

Software 10

Cambiare il mezzo di installazione 11

YaST Online Update (YOU) 11

Installare/disinstallare del software 12

Update del sistema 14

Patch-CD-Update 15

Hardware 15

Stampante 15

Dispositivi di input e visualizzazione (SaX2) 15

Informazione hardware 16

Rete/Base 16

Configurazione della scheda di rete 16
E-mail 17
Rete/Avanzata 17
Configurare un server NFS 17
Configurare NIS 18
Configurare hostname e DNS 18
Configurare il routing 19
Sicurezza e utente 19
Amministrazione degli utenti 19
Amministrazione gruppi 20
Impostazioni di sicurezza 20
Firewall 22
Sistema 24
Creare un backup del sistema 24
Ripristina sistema 25
Editor per sysconfig 26
Editor dei runlevel 26
Partizionatore 27
Logical Volume Manager (LVM) 27
Soft-RAID 28
Selezionate il fuso orario 30
Selezione della lingua 30
Misc 30
Log di avvio 30
Log di sistema 30
Carica il CD dei driver del produttore 31

3 Il sistema X Window **33**
Un pò di storia 33
La versione 4.x di XFree86 34
Configurazione con SaX2 35
SaX2: la finestra principale 36
Display 37
Scheda grafica 38
Colori/Definizione/i) 38
Accelerazione tridimensionale 39
Posizione e dimensioni dello schermo 39
Multihead 40
Dispositivi di immissione 40
AccessX 42
Come ottimizzare l'installazione del sistema X Window 43
Inserire altri font (TrueType) 49

4 Stampare **53**
Principi 54
Premesse 57
Configurare la stampante con YaST2 61
Queue e configurazione 61
I principi della configurazione della stampante di YaST2 62
Configurazione automatica 64
Configurazione manuale 65
Configurazione per applicativi 69
Stampare sulla riga di comando 69
Con il sistema di stampa LPRng/lpdfilter 69
Con il sistema di stampa CUPS 69
Configurazione manuale di porte di stampanti locali 70
Porte parallele 70
Collegamento USB 73
Interfaccia della stampante IrDA 75

Interfaccia seriale 76
Configurazione manuale di LPRng/lpdfilter 76
Lo spooler di stampante LPRng/lpdfilter 77
Tool di riga di comando per il LPRng 78
Per queue locali 78
Per queue remote 81
Il filtro della stampante del sistema di stampa LPRng/lpdfilter 83
Generare propri filtri di stampante per lo spooler della stampante 92
Il sistema di stampante CUPS 96
Terminologia 96
IPP e server 96
Configurazione del server CUPS 97
Stampante di rete 99
Elaborazione interna dell'incarico 99
Suggerimento 101
Tool della riga di comando per il sistema di stampa CUPS 103
Per queue locali 103
Queue remote 106
Su Ghostscript 107
a2ps 111
Convertire in PostScript con psutils 113
psnup 113
pstops 114
psselect 117
Verifica allo schermo con Ghostscript 118
La codificazione di testi ASCII 119
Stampare nella rete TCP/IP 121
Denominazione 121
Risolvere dei problemi 129
Server della stampante LPD ed IPP 132
Solo con CUPS 132
LPRng/lpdfilter e CUPS 133

II System **135**

5 Il Kernel **137**

Le sorgenti del kernel . . . 137

Moduli del kernel . . . 138

6 Particolarità del sistema **141**

Gli standard Linux . . . 142

Filesystem Hierarchy Standard (FHS) . . . 142

Linux Standard Base (LSB) . . . 142

teTeX – TeX su SuSE Linux . . . 142

Esempi di ambienti per FTP ed HTTP . . . 142

Informazioni su pacchetti speciali di software . . . 143

Il pacchetto bash ed /etc/profile . . . 143

Il pacchetto cron . . . 144

File di log – il pacchetto logrotate . . . 144

Pagine di manuale . . . 146

Il comando ulimit . . . 146

Il comando free . . . 147

Il file /etc/resolv.conf . . . 147

Console virtuali . . . 148

Mappatura della tastiera . . . 148

Adattamenti locali – I18N/L10N . . . 149

7 Supporto per programmi a 32 bit e a 64 bit in un ambiente a 64-bit **153**

Introduzione . . . 154

Supporto runtime . . . 154

Lo sviluppo di software . . . 155

Il kernel . . . 156

8 Il concetto di "boot" 159
Il programma init 160
I runlevel 160
Passaggio di runlevel 162
Gli script init 163
Il Runlevel Editor di YaST2 166
SuSEconfig, /etc/sysconfig e /etc/rc.config 167
Configurazione di sistema con l'editor Sysconfig di YaST2 168
Script e variabili: configurazione del sistema 169

III Networking 201

9 Fondamenti del collegamento in rete 203
TCP/IP: il protocollo usato da Linux 204
Modelli a strati 205
Indirizzi IP e routing 207
Sistema nome di dominio 211
IPv6 – l'Internet di prossima generazione 212
Perché un nuovo protocollo Internet? 212
Configurazione di un indirizzo Ipv6 214
Maschere di rete Ipv6 216
Documentazione e link su IPv6 216
L'integrazione nella rete 218
Premesse 218
Configurazione con YaST2 218
Configurare IPv6 220
Configurazione manuale della rete 221
File di configurazione 221
GLi script startup 227
Il routing con SuSE Linux Enterprise Server 228
DNS – Domain Name Service 230
Inizializzare il name server BIND 230

Il file di configurazione /etc/named.conf 232
Ulteriori informazioni 239
NIS – Network Information Service 240
Server NIS master e slave 240
Il modulo client NIS in YaST2 242
Configurazione manuale di un client NIS 243
NFS – filesystem ripartiti 245
Importare filesystem con YaST2 245
Importare manualmente i filesystem 245
Esportare filesystem con YaST2 246
Esportare manualmente i filesystem 246
DHCP 250
Il protocollo DHCP 250
I pacchetti software DHCP 250
Il server DHCP, dhcpd 251
Computer con indirizzo IP fisso 253
Ulteriori fonti di informazione 254

10 Reti eterogenee **255**
Samba 256
Installazione e configurazione del server 257
Samba come server per il login 261
Installazione dei client 262
Ottimizzazione 263
Netatalk 263
Configurazione del file server 264
Configurazione del server della stampante 268
Inizializzare il server 269

11 Internet **271**
Server proxy: Squid . . . 272
Cos'è una Proxy-Cache? . . . 272
Informazioni sulla cache proxy . . . 272
Requisiti di sistema . . . 274
Avviare Squid . . . 276
Il file di configurazione /etc/squid.conf . . . 278
Configurazione del proxy trasparente . . . 283
Squid e altri programmi . . . 285
Altre informazioni su Squid . . . 290

12 Reti sicure **291**
Masquerading e Firewall . . . 292
I principi del masquerading . . . 292
Basi del firewall . . . 294
SuSEfirewall2 . . . 295
SSH – secure shell, l'alternativa sicura . . . 297
Il pacchetto OpenSSH . . . 298
Il programma ssh . . . 298
scp – copiare in modo sicuro . . . 299
sftp - trasmissione più sicura . . . 299
Il demone SSH (sshd): la parte del sever . . . 300
SSH-meccanismi di autenticazione . . . 301
Deviazione di X, dell'autenticazione ed altre deviazioni . . . 302
Autenticazione della rete — Kerberos . . . 303
La terminologia di Kerberos . . . 304
Come funziona? . . . 305
Kerberos e l'utente . . . 308
Ulteriori informazioni su Kerberos . . . 309
Installare e amministrare Kerberos . . . 310
Selezionare i realm di Kerberos . . . 310
Impostare l'hardware KDC . . . 311

Sincronizzazione dell'orologio 312
Configurazione di log 313
Installare il KDC 313
Configurare client Kerberos 317
Gestire i principal 319
Abilitare il supporto PAM per Kerberos 320
Configurare un server di rete per Kerberos 324
Configurare sshd per l'autenticazione Kerberos 325
Usare LDAP e Kerberos 325

A Manual-Page di e2fsck **327**

B La Licenza Pubblica GNU (GPL) **333**

Bibliografia **343**

Parte I

Configuration

YaST2 nel modo testo (ncurses)

YaST2 può essere usato anche tramite un terminal basato su testo. Questo si rivela utile se l'amministratore non dispone di un accesso su una superficie grafica X11.

L'uso

Per lanciare YaST2 nel modo testo, immettete `yast` come `root` in un terminale.

Forse risulta essere un pò inconsueto ma è molto facile destreggiarsi in YaST nel modo di testo. Con i tasti (Tab), (Alt) + (Tab), (Spazio), tasti freccia ((↑) e (↓)) ed (Enter) nonché gli shortcut si lascia maneggiare in fin dei conti l'intero programma. Se avviate YaST2 nel modo testo apparirà come prima il centro di controllo di YaST2 come indicato nella figura 1.1.

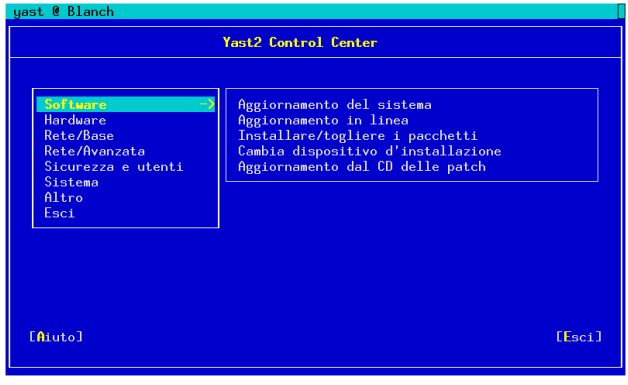


Figura 1.1: *La finestra principale del centro di controllo di YaST2*

La finestra è suddivisa in tre settori: nella colonna sulla sinistra vedete le categorie a cui appartengono i diversi moduli. La categoria delle selezioni quando è attivate è marcata da una cornice bianca. La categoria selezionata, attiva si riconosce dalla striscia con cui viene evidenziata. I moduli corrispondenti della categoria attiva vengono elencati nella casella sulla destra. In basso, vedete i bottoni 'Aiuto' e 'Esci'.

Dopo l'avvio del centro di controllo di YaST2 è la categoria 'Software' ad essere selezionata. Con i tasti freccia (↑) e (↓) potete passare da una categoria all'altra. Con (→) passata alla selezione dei moduli appartenenti alla categoria. La casella dei moduli viene evidenziata e con i tasti (↑) o (↓) potete passare da un modulo all'altro. Quando un modulo è selezionato, esso viene evidenziato con una barra colorata e un breve testo che descrive il modulo viene visualizzato in basso nella finestra.

Premendo su (Enter) il modulo selezionato viene lanciato. Diversi bottoni o campi di selezione contengono una lettera di un altro colore (gialla di default). Con la combinazione (Alt) + (lettera gialla) selezionate il bottone corrispondente direttamente.

Con 'Esci' lasciate il centro di controllo di YaST2 oppure selezionando la voce 'Esci' nella categoria delle selezioni e premendo (Enter).

Restrizioni riguardanti la combinazione dei tasti

Se sul vostro sistema avete delle combinazioni di tasti con (Alt) e il X server è in esecuzione può verificarsi che queste combinazioni di tasti non funzionino in YaST2. Inoltre può darsi che dei tasti come (Alt) o (⇑) siano già configurati (mappati) dalle impostazioni del terminale che usate.

Sostituire (Alt) con (Esc): Le combinazioni con Alt possono essere eseguiti con (Esc) al posto di (Alt), per esempio (Esc) + (h) al posto di (Alt) + (h).

Spostarsi in avanti o indietro con (Ctrl) + (f) e (Ctrl) + (b): Se le combinazioni con (Alt) e (⇑) sono stati già mappati dal window manager o dal terminale, avete la possibilità di usare (Ctrl) + (f) (avanti) (Ctrl) + (b) (indietro).

Usare i moduli

Nel seguente paragrafo si parte dal presupposto, per maggior chiarezza, che le combinazioni con (Alt) funzionino.Se necessario, provvedete a fare le sostituzioni appropriate o usate una console puramente testuale.

Navigare tra i bottoni/liste di selezione: Per scorrere i bottoni e/o le liste di selezione usate rispettivamente i tasti (Tab) e (Alt) + (Tab).

Navigare nella lista di selezione: Con i tasti freccia ((↑) e (↓)) selezionate i singoli elementi nel riquadro attivo in cui si trova una lista di selezione, per esempio i singoli moduli di un gruppo di moduli nel centro di controllo.

Marcare radio bottoni e check box Per selezionare bottoni con una parentesi quadra vuota (check box) o parentesi tonda (radio bottoni) usate (Spazio) o (Enter). Per selezionare i bottoni nel margine inferiore dei singoli moduli o del centro di controllo premete (Enter), quando sono già marcati (color verde), o eseguite la selezione con la combinazione (Alt) + (tasto_giallo) (cfr. Fig. 1.2).

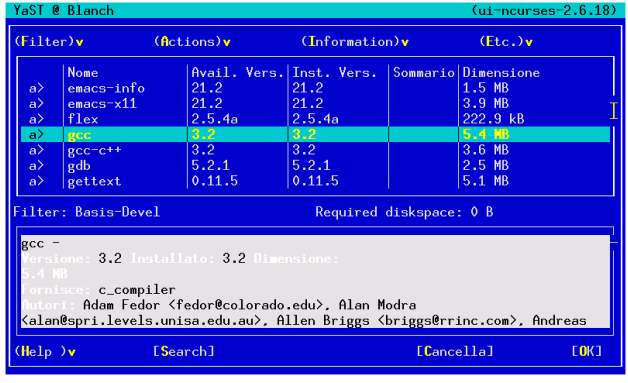


Figura 1.2: *Il modulo per l'installazione del software*

Richiamare singoli moduli

Per risparmiare del tempo, ogni modulo di YaST2 può essere richiamato singolarmente, basta immettere: `yast` ⟨*`module name`*⟩. l modulo di rete per esempio

si avvia con il comando `yast lan`. Una lista dei nomi dei moduli che sono disponibili nel vostro sistema, si ottiene con `yast -l` o `yast --list`.

YOU: YaST Online Update

Potete richiamare e gestire anche YOU (YaST Online Update) dalla console. Trovate le istruzioni nel capitolo *Aggiornamento in linea dalla console* a pagina 11. L'amministratore può impostare un cosiddetto cron job settimanale, in modo da aver un sistema sempre aggiornato grazie a YOU.

Il cron job per YOU

Visto che non tutti che vogliono/devono usare YOU, sanno anche come impostare un cron job, segue una breve descrizione del processo. In linea di massima esistono due possibilità per farlo, riportiamo di seguito quella più semplice :

1. Diventate root
2. Avviate il crontabeditor con il comando `crontab -e`.
3. Premete la lettera `i` per la modalità di inserimento in vi
4. Inserite le seguenti righe:

   ```
   MAILTO=" "
   13 3 * * 0 /sbin/yast2 online_update auto.get
   53 3 * * 0 /sbin/yast2 online_update auto.install
   ```

   I primi 5 caratteri delle righe inferiori vanno lette da sinistra a destre e stanno per: 13=minuti, 3=ore, *=giorno del mese, non fa differenza, *=mese dell'anno, non fa differenza, 0=domenica. Dunque significa che la prima registrazione inizializza il cron job ogni domenica alle 3 e 13 di notte. La seconda dopo 40 minuti, alle 3 e 53. La riga `MAILTO=" "` impedisce che root riceva l'output di YaST2-ncurses come e-mail e può essere naturalmente omessa.

   Attenzione

   Immettete degli orari per i cron job, però non quello riportato nell'esempio, altrimenti, a quell'ora il server ftp è sovraccarico o viene superato il numero massimo degli accessi contemporanei consentiti.

   Attenzione

5. Salvate il cron job con (immettendo l'uno dopo l'altro) Esc `:wq` oppure con Esc ZZ.

Il demone di cron viene automaticamente riavviato e il vostro cron job viene registrato nel file `/var/spool/cron/tabs/root`

YaST2 nel modo grafico

Con l'aiuto di YaST2, potrete arricchire il vostro sistema SuSE Linux Enterprise Server di altri componenti hardware (stampante, scheda audio, ecc.), servizi di sistema e Internet account, nonché configurare, installare o eliminare singoli pacchetti di software.

Inizializzare YaST2 10
Software 10
Hardware 15
Rete/Base 16
Rete/Avanzata 17
Sicurezza e utente 19
Sistema 24
Misc 30

Inizializzare YaST2

YaST2 si avvia nel modo grafico tramite il sistema di menù di KDE, che potete dirigere sia con il mouse che con la tastiera.

Dopo la sua inizializzazione appare il centro di controllo di YaST2 Sulla sinistra, troverete una suddivisione in 'Hardware', 'Rete/Base', 'Rete/Avanzata', 'Sicurezza/Utente', 'Software', 'Sistema' e 'Altro'. Cliccando su una delle icone, apparirà il contenuto corrispondente ad ogni categoria nella parte destra della finestra. La configurazione consiste solitamente di più passi.

Selezionando 'Avanti', YaST2 vi assisterà in ogni dialogo. Nella schermata sulla sinistra, potrete leggere un testo di aiuto per ognuna delle fasi dell'installazione, che vi spiegherà cosa inserire di volta in volta.

Dopo aver digitati i parametri del caso, chiudete il processo cliccando 'Fine' nell'ultimo dialogo di configurazione. La configurazione verrà quindi memorizzata.

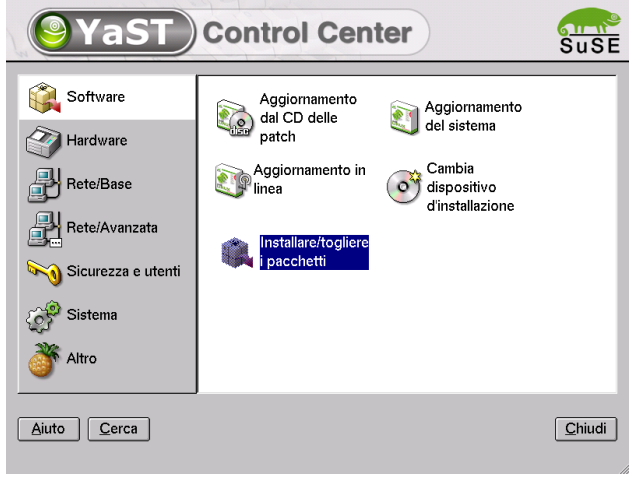


Figura 2.1: *YaST2: amministrazione e configurazione del sistema*

Software

Con questo modulo potrete installare o eliminare singoli pacchetti di software o addirittura cambiare il mezzo di installazione. Troverete anche due strumenti di

attualizzazione: uno per l'attualizzazione "normale" e uno per l'attualizzazione online tramite il nostro server FTP.

Cambiare il mezzo di installazione

Sul mezzo di installazione si trova la software da installare. Si può installare dal CD (la via più comune), da un server di rete o dal disco rigido. (Per maggiori dettagli vedi il manuale di *Installazione* di SuSE Linux Enterprise Server ed i testi esplicativi di YaST2).

Quando uscite dal modulo con 'Finisci', le impostazioni vengono salvate e applicate ai moduli di configurazione 'Installa/elimina software' e 'Aggiornamento del sistema'. Questo modulo vi offre inoltre la possibilità di procedere con 'Installa' per installare o eliminare dei pacchetti.

YaST Online Update (YOU)

L'aggiornamento in linea di YaST permette di installare importanti upgrade ovvero delle ottimizzazioni. Sul server FTP di SuSE trovate le relative "patch" da scaricare. I pacchetti possono essere installati in modo del tutto automatico. Con 'Aggiornamento manuale' avete adesso la possibilità di stabilire quale patch deve essere installata sul vostro sistema SuSE Linux Enterprise Server.

Fate clic su 'Dettagli' per avere maggiori informazioni sull'ultimo aggiornamento e pacchetti disponibili il cui contenuto si lascia visualizzare facendo clic su 'Mostra informazioni sulle patch'.

Con 'Prossimo' scaricate l'elenco della patch disponibili (se avete selezionato 'Aggiornamento manuale'). Ora parte il modulo per l'installazione del software (vedi *Installare/disinstallare del software* nella pagina successiva), elencando le patch scaricate. Qui potete scegliere i pacchetti da installare. Potete anche semplicemente accettare la proposta di installazione di YaST2. Il processo di aggiornamento in linea si conclude facendo clic su 'Prossimo' oppure 'Fine'.

Aggiornamento in linea dalla console

Per gli amministratori di sistema sussiste inoltre la possibilità di eseguire l'aggiornamento in linea tramite la shell. Digitando come `root` il comando

```
terra:/root #  yast2 online_update .auto.get
```

scaricate la lista delle patch attuale e tutti i relativi .rpm dal primo server nella lista `/etc/suseservers`. Se vi interessano solo determinate patch, potete aggiungere delle opzioni al comando.

Le opzioni possibili sono `security`, `recommended`, `document`, `YaST2` ed `optional`. `security` scarica solo patch concernenti la sicurezza, `recommended` gli update consigliati da SuSE, `document` vi fornisce delle informazioni sulle patch o sul server FTP, `YaST2` scarica solo patch di YaST2 e `optional` fornisce degli update non di primaria importanza.

Le informazioni sulle patch sono memorizzate sotto `/var/lib/YaST2/you/<basearch>/update/<productname>/<version>/patches`. Possono essere letti solo da `root`. ⟨*X.Y*⟩ indica la versione di SuSE Linux.

Il comando per scaricare le patch di sicurezza:

```
terra:/root #  yast2 online_update .auto.get security
```

Ogni volta che immettete `.auto.get` normalmente la lista dei server FTP viene copiata sotto `/etc/suseservers`. Se non volete che ciò avvenga, dovete disabilitare questa funzione nel file `/etc/sysconfig/onlineupdate`. Per fare ciò la riga `YAST2_LOADFTPSERVER="yes"`. `yes` va impostata su `no`. Installate ora la patch con

```
terra:/root #  yast2 online_update .auto.install
```

Questo comando installa le patch che avete selezionato. Se volete installare solo un gruppo, potete utilizzare le stesse opzioni descritte per `.auto.get`.

Questo metodo ha il vantaggio che può essere automatizzato. L'amministratore di sistema può scaricare i pacchetti per esempio durante la notte e installare quelli che necessità la mattina.

Installare/disinstallare del software

Questo modulo vi permette di installare, aggiornare o disinstallare del software sul vostro computer. Per eseguire l'installazione dal CD, inserite il CD nel lettore

Il filtro delle selezioni

Nella finestra principale, a sinistra in alto sotto 'Filtro' potete scegliere il criterio in base al quale vengono mostrati i pacchetti da selezionare. Il valore predefinito è 'Gruppi pacchetto'.

Se usate il filtro 'Gruppi di pacchetti' i gruppi verranno visualizzati sulla sinistra in una struttura ad albero. Se fate clic sul termine principale (per esempio 'Sviluppo' o 'Documentazione'), appariranno nella finestra in alto a destra tutti i pacchetti di software appartenenti a questo gruppo. Se fate clic su un

sottogruppo, vedrete a destra solo i pacchetti appartenenti al corrispondente sottogruppo.

Un'altra possibilità interessante è rappresentata dal filtro 'Selezioni'. Avrete incontrato questo filtro durante l'installazione se avete impostato il software nella schermata proposta. Con 'Selezioni' potete, con un semplice clic, avviare l'installazione o la disinstallazione di una scelta predefinita di pacchetti per determinati campi di applicazione. Questo è l'unico filtro che vi consente già adesso di abilitare delle voci sulla sinistra. Se fate clic sulle caselle delle selezioni, verranno installati tutti i pacchetti della selezione. Se dalla selezione di default per esempio togliete KDE, alla conferma verranno deinstallati tutti i pacchetti di KDE. I pacchetti di ogni selezione vengono mostrati a destra con il relativo stato. Chiaramente anche qui potrete selezionare e deselezionare i singoli pacchetti secondo le vostre preferenze. Le selezioni predefinite includono 'Sviluppo avanzato', 'Tutto KDE' o 'Server web'.

La finestra dei pacchetti

Qui viene mostrato lo stato del pacchetto: il nome del pacchetto, una breve descrizione, la dimensione, la versione e la colonna dei sorgenti dove potete stabilire se installare anche il sorgente del pacchetto.

Diverse icone indicano lo stato del pacchetto. Un pacchetto può avere i seguenti stati:

- è installato
- non è e non viene installato
- viene installato attraverso la selezione a mano
- viene installato, perché richiesto da un altro pacchetto selezionato (dipendenze)
- viene sostituito da una nuova versione (aggiornamento)
- viene cancellato (deinstallato)
- "taboo": evita che dei pacchetti selezionati automaticamente a causa di una dipendenza da altri pacchetti vengano installati (consigliato solo per esperti)
- bloccato: evita che il pacchetto venga aggiornato o cancellato (utile per pacchetti che sono stati compilati manualmente o che provengono da una fonte diversa).

- rinominato: questo stato non può essere selezionato manualmente (nei casi in cui un pacchetto è stato aggiornato e il nuovo pacchetto ha un nome diverso)

Facendo clic sulle icone a sinistra dei nomi dei pacchetti potete passare da uno stato all'altro. Potrete scegliere solo tra stati che hanno senso, cioè un pacchetto non installato per esempio non può assumere lo stato "Cancellare".

Attenzione

Avete la possibilità di contrassegnare dei pacchetti installati che intendete cancellare. Leggete attentamente gli avvertimenti del sistema e non cancellate alcun pacchetto incluso del sistema di base di Linux.

Attenzione

La finestra info

In basso a destra vedete una finestra con delle linguette che vi forniscono informazioni sul relativo pacchetto: una descrizione dettagliata, dati tecnici, un elenco di file che sono stati installati con questo pacchetto, i pacchetti che sono necessari per questo pacchetto, i pacchetti che richiedono questo pacchetto ed eventuali conflitti con pacchetti installati o selezionati per essere installati.

Cerca

Andando su 'Cerca' potete avviare una ricerca mirata di nomi di pacchetti o parte dei nomi. In seguito potete stabilire cosa debba succedere con i pacchetti trovati.

Update del sistema

Questo modulo vi permette di aggiornare il vostro sistema. YaST2 determina quali pacchetti sono da aggiornare oppure potete decidere voi quali pacchetti aggiornare.

Questa funzione si rivela particolarmente utile se un file binario è stato eliminato accidentalmente. Il modulo dell'aggiornamento elencherà i pacchetti software appropriati e le marcherà per l'update. In questo modo la ricerca del software appropriato, che spesso richiede tanto tempo, viene viene eseguita in modo automatico.

Patch-CD-Update

A differenza dell'aggiornamento in linea le patch non si trovano sul server ftp, ma sul CD.

Una volta inserito il CD con le patch, vi verranno mostrate, nella maschera di questo modulo di YaST2, tutte le patch che si trovano sul CD. Da questa lista potrete selezionare quelle da installare. Se avete dimenticato di inserire il CD nel dispositivo di lettura, ve lo comunicherà il sistema. Inserite il CD e ricominciate l'aggiornamento.

Hardware

Il nuovo hardware dovrà essere, per prima cosa, installato e connesso al sistema secondo le istruzioni del produttore. Accendete i dispositivi esterni, stampante o modem, e aprite il modulo YaST2 corrispondente. Gran parte dei dispositivi in commercio verrà riconosciuto automaticamente da YaST2 che farà comparire i dati tecnici sullo schermo. Nel caso l'identificazione automatica fallisca, YaST2 vi riporta una lista di dispositivi hardware, (per esempio modello/produttore), da cui potrete selezionare la voce corrispondente alla vostra marca.

Alla voce 'Hardware', troverete degli strumenti di configurazione per l'installazione di diversi tipi di hardware. Se il vostro hardware è stato automaticamente riconosciuto da YaST2 troverete i dati tecnici relativi consultando le informazioni hardware.

Stampante

Con questo modulo potete configurare le stampanti collegate al vostro sistema. Per ulteriori informazioni vedi il *Stampare* a pagina 53.

Dispositivi di input e visualizzazione (SaX2)

Questo modulo configura l'interfaccia grafica X11 e i dispositivi di input su sistemi che supportano una interfaccia grafica. Potete utilizzare questo modulo anche per ritoccare la configurazione di X11 esistente (p.e. la profondità dei colori).

Informazione hardware

YaST2 esegue il rilevamento hardware ai fini della configurazione dei componenti hardware. I dati tecnici rilevati vengono mostrati in questa schermata.

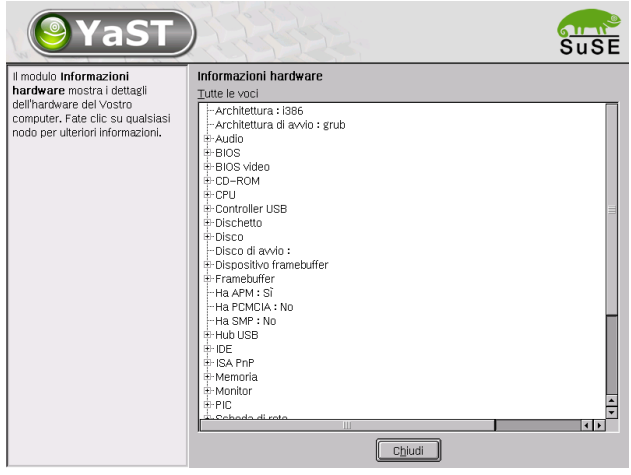


Figura 2.2: *Visualizzazione dell'informazione hardware*

Rete/Base

Qui YaST2 vi mette a disposizione gli strumenti di configurazione basilari che vi spianano la via per entrare in Internet, ovvero tool per configurare la scheda di rete, host name e DNS. Anche il routing si lascia configurare con questo modulo.

Configurazione della scheda di rete

Con questo modulo di YaST2 potete configurare la vostra scheda di rete per una connessione ad una rete locale o ad Internet. Il procedimento da seguire è descritto nel capitolo *L'integrazione nella rete* a pagina 218.

E-mail

Il modulo di configurazione per le impostazioni e-mail è stato adattato alle richieste attuali. Oltre a sendmail è supportato anche postfix per l'invio di e-mail. Nella finestra della configurazione sotto 'Rete/Avanzato' selezionate il vostro tipo di collegamento:

'Computer con connessione permanente' In questo caso si parla di "linea fissa" che viene spesso utilizzata da aziende e istituzioni varie che usano intensivamente Internet e sono permanentemente connessi ad Internet. Questa voce del menu vale anche per gli utenti di una rete locale, senza connessione permanente, però con un server di posta elettronica centrale per l'invio di e-mail.

'Computer con connessione temporanea (modem od ISDN)' Sarà il caso della maggior parte degli utenti che a casa hanno un PC non collegato ad alcuna rete che ogni tanto si connettono ad Internet – tramite modem, DSL/ADSL o ISDN.

'Nessuna connessione' Se non potete accedere ad Internet e non siete collegati ad alcuna rete, chiaramente non potrete inviare o ricevere delle e-mail.

In seguito dovete selezionare un provider per l'invio di e-mail e registrare almeno un utente locale. Se avete una connessione "dial–up", potete indicare diversi server POP per la ricezione delle e-mail per diversi utenti.

Potete anche facoltativamente stabilire dei nomi alias, il mascheramento dell'indirizzo o dei domini virtuali. Con 'Fine' concludete la configurazione.

Rete/Avanzata

Per amministratori di rete esistono moduli per avviare e fermare servizi di sistema come inetd, Sendmail (con configurazione per esperti), per client e server NFS, routing e client NIS. 'Rete avanzata' offre le stesse funzionalità di 'Configurazione scheda di rete' di 'Rete/Base', in modo da poter configurare qui altre interfacce di rete come il modem.

Configurare un server NFS

Con YaST2 potete trasformare velocemente un computer della vostra rete in un server NFS. Si tratta di un server che mette a disposizione directory e file

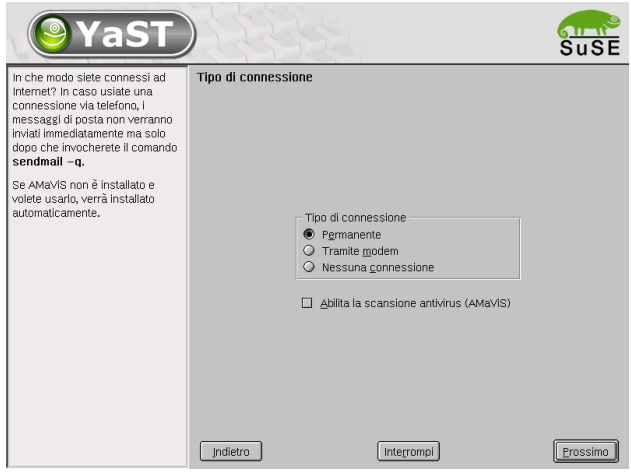


Figura 2.3: *Configurazione e-mail*

a tutti i computer che hanno il permesso di accesso. Potete mettere a disposizione degli utenti tanti applicativi senza dovere installarli localmente su ogni computer

Per i dettagli sulla configurazione del sistema come server NFS andate alla sezione *NFS – filesystem ripartiti* a pagina 245.

Configurare NIS

Non appena diversi sistemi Unix in una rete vogliono accedere a risorse condivise, deve essere assicurato per tutti gli host che le ID degli utenti e dei gruppi non entrano in conflitto. La rete deve essere trasparente per l'utente ed indipendentemente dall'host, l'utente dovrà trovare sempre lo stesso ambiente.

Leggete la sezione *NIS – Network Information Service* a pagina 240 per sapere come configurare NIS come client e come server.

Configurare hostname e DNS

Qui vengono impostati il nome host e i dati DNS del sistema. Dovreste evitare di modificare in seguito queste informazioni, poiché si tratta di parametri necessari per il funzionamento della rete. Leggete il capitolo *L'integrazione nella rete* a pagina 218 e *DNS – Domain Name Service* a pagina 230 a riguardo.

Configurare il routing

Il routing è anche un parametro importante per la configurazione della rete. Nel capitolo *L'integrazione nella rete* a pagina 218 viene spiegato in modo dettagliato il routing su Linux.

Sicurezza e utente

Amministrazione degli utenti

Selezionate 'Modifica e crea utenti' . YaST2 vi offre una lista di tutti gli utenti per aiutarvi nell'amministrazione degli utenti. Per rimuovere un utente fate semplicemente clic sulla lista in modo da evidenziare l'utente in questione e quindi fate clic su 'Rimuovi'. Per aggiungere un utente immettete semplicemente le informazioni richieste nelle caselle corrispondenti. Dopo il nuovo utente può entrare nel sistema digitando login e password. Impostate i dettagli sotto 'Modifica' → 'Dettagli'.

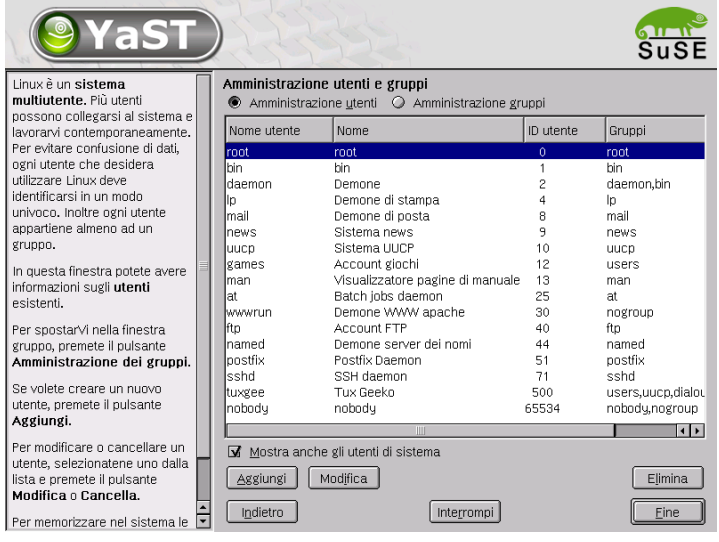


Figura 2.4: *Amministrazione utenti*

Amministrazione gruppi

Selezionate ‘Modifica e crea gruppi’. YaST2 vi mette a disposizione una lista di tutti i gruppi per aiutarvi nell’amministrazione dei gruppi. Per rimuovere un gruppo, fate clic sul gruppo nella lista (la riga corrispondente verrà evidenziata in blu scuro), poi fate clic su ‘Rimuovi’. Per ‘Aggiungere’ o ‘Modificare’ un gruppo basta semplicemente seguire i testi esplicativi di YaST2.

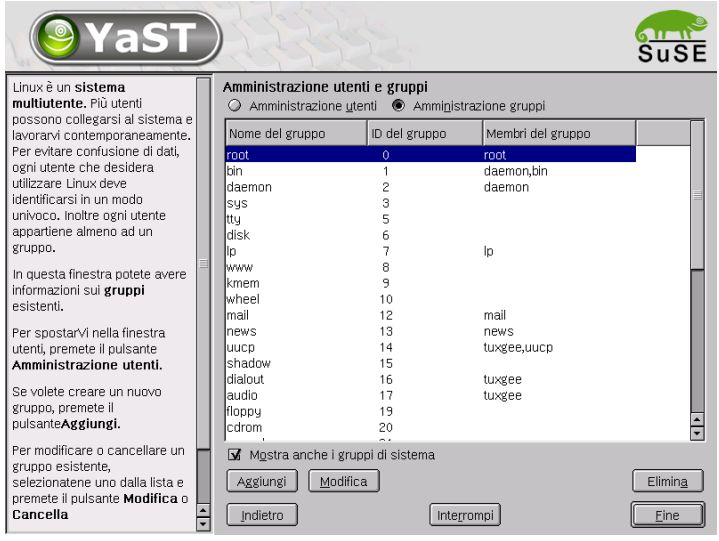


Figura 2.5: *Amministrazione gruppi*

Impostazioni di sicurezza

Nel menù iniziale ‘Configurazione della sicurezza locale’, che potete trovare sotto ‘Utenti e sicurezza’, ci sono quattro possibilità:

Livello 1 è indicato per i computer non collegati in rete (preconfigurato), Livello 2 per i computer collegati in rete (preconfigurato), Livello 3 per i server collegati in rete (preconfigurato) e personalizzato per le vostre impostazioni personalizzate.

Se fate clic su una delle tre voci, avete la possibilità di incorporare uno dei livelli di opzioni di sicurezza preconfigurate. Per farlo, fate clic su ‘Fine’. Sotto

'Dettagli' potete accedere alle singole impostazioni per modificarle. Se sceglietе 'Definito dall'utente', verrete condotti automaticamente alle varie finestre di dialogo tramite 'Avanti'. Qui potete trovare i valori di installazione predefiniti.

'Impostazioni password' Potete definire la lunghezza della password per i futuri utenti (lunghezza minima e massima). Un'impostazione ragionevole è da cinque a otto caratteri. Impostate la durata della validità della password, la data di scadenza e con quanti giorni di anticipo bisogna avvisare l'utente della scadenza della password (l'utente viene avvisato quando accede alla console testuale).

'Impostazioni di avvio' In questa schermata impostate come va interpretata la combinazione tasti (Ctrl) + (Alt) + (Canc) Di solito sulla console si riavvia il sistema Non modificate impostazione a meno che la vostra macchina o server sia accessibile pubblicamente e temete che qualcuno possa eseguire questa operazione senza essere autorizzato. Se selezionate 'Arresta', il sistema si arresterà. Con 'Ignora', questa combinazione di tasti verrà ignorata. Inoltre potete impostare chi ha il permesso di spegnere il sistema da KDM (KDE Display Manager — il login grafico). Le opzioni sono 'Solo root' (Amministratore di sistema), 'Tutti gli utenti', 'Nessuno', o 'Utenti locali'. Se selezionate 'Nessuno' il sistema può essere spento solo tramite la console.

'Login' Tipicamente, subito dopo un tentativo di login fallito, c'è un periodo di attesa di qualche secondo prima che sia possibile un nuovo login. Lo scopo di questo periodo di attesa è di rendere più difficile ai malintenzionati indovinare la vostra password provandola più volte. Inoltre, avete la possibilità di attivare le voci 'Registra i tentativi di login falliti' e 'Registra i tentativi di login riusciti'. Se sospettate che qualcuno stia cercando di scoprire la vostra password, controllate i file di log in `/var/log`.

'Impostazioni aggiunta utenti' Ogni utente ha un codice identificativo sia numerico che alfabetico. La corrispondenza tra questi due codici è stabilita dal file `/etc/passwd` e dovrebbe essere il più univoca possibile.

Usando i dati in questa schermata, definite l'intervallo di numeri assegnabili alla parte numerica del codice identificativo utente quando viene creato un nuovo utente. L'impostazione standard è 500 e non dovrebbe venire diminuita.

'Impostazioni varie' 'Facile', 'Sicuro' e 'Paranoico'. La prima dovrebbe essere sufficiente per la maggior parte degli utenti. La guida di YaST2 vi fornirà informazioni sui tre livelli di sicurezza.

L'impostazione 'Paranoico' è estremamente restrittiva e dovrebbe essere usata come punto di partenza per le impostazioni decise dall'amministratore di sistema. Se scegliete 'Paranoico', tenete presente che potrebbero verificarsi dei problemi o malfunzionamenti durante l'uso di certi programmi, perché non avrete più i diritti di accesso ad alcuni file.

Inoltre, in questa finestra, potete definire quali utenti possono invocare il programma "updatedb". Questo programma, che viene eseguito quotidianamente oppure subito dopo l'avvio, genera un database (locatedb) in cui viene memorizzata la posizione di ogni file nel vostro computer (locatedb può essere consultato usando il comando `locate`). Se selezionate 'Nessuno', qualsiasi utente può trovare solo i percorsi nel database che possono essere visti da qualsiasi altro utente (non privilegiato). Se selezionate `root`, tutti i file locali possono venire catalogati, perché l'utente `root`, come superutente, può accedere a tutte le directory.

Un'altra opzione è di attivare la voce 'Togli la directory attuale dal path dell'utente root', una scelta ragionevole. Infine, avete l'opzione 'Disabilita il login tramite telnet per l'utente root'. È una buona idea scegliere anche questa opzione. In caso contrario, qualsiasi utente nella rete può collegarsi al vostro computer come `root` tramite telnet, attraverso il quale la password di root viene trasmessa in chiaro (non cifrata).

Con 'Fine', questa configurazione viene terminata.

Firewall

Con questo modulo diventa un gioco da ragazzi abilitare e configurare il SuSE Firewall. Se siete collegati ad Internet dovreste fare uso di questa misura protettiva. Il SuSE Firewall offre efficace protezione.

Questo modulo consta di quattro dialoghi. Nel primo, dovete selezionare l'interfaccia da proteggere (vd. figura 2.7 a pagina 24). 'Interfaccia esterna' è l'interfaccia per l'Internet. 'Interfaccia interna' serve solo se vi trovate in una rete interna e volete usare il firewall per proteggere il vostro computer contro attacchi provenienti dall' interno. In questo caso il vostro computer si troverebbe in una "demilitarized zone" (DMZ). Di solito una configurazione con DMZ si ha solo per reti aziendali.

Dopo aver selezionato l'interfaccia, attivate selettivamente i servizi del vostro computer per i quali permettere l'accesso da Internet (vd. figura 2.8 a

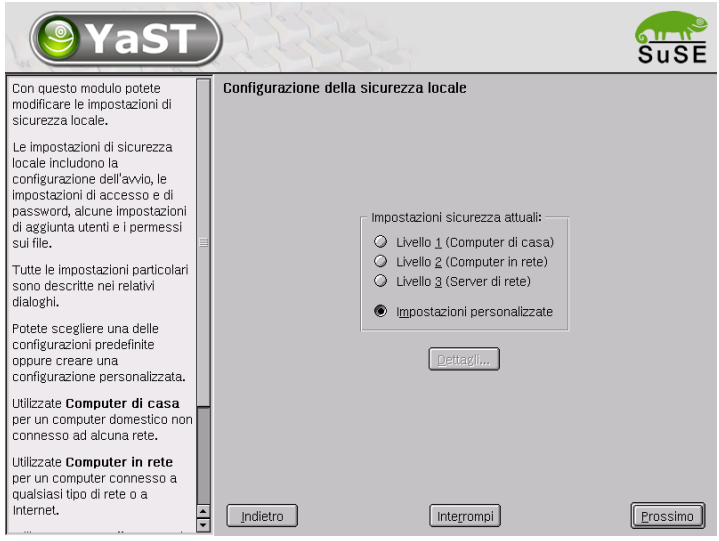


Figura 2.6: *Impostazioni sicurezza*

pagina 25). Se non usate un server con uno di questi servizi ma volete solo navigare su Internet ed inviare e ricevere e-mail non attivate alcun dei servizi elencati; vale la regola: meno “porte” sono accessibili dall‘esterno e minore è il rischio di intrusioni).

Se i termini mascheramento e traceroute non vi sono noti, accettate semplicemente il terzo dialogo senza modificarlo. Potete anche accettare il dialogo finale dato che le opzioni di registrazione predefinite di solito si rivelano essere sufficienti.

Se fate clic su ‘Prossimo’, una piccola finestra vi chiede la conferma. In seguito la nuova configurazione viene salvata sul disco. Al prossimo collegamento ad Internet, il vostro computer è protetto in modo efficace contro intrusioni e attacchi.

Per ulteriori informazioni su SuSE Firewall, vedi capitolo *Masquerading e Firewall* a pagina 292.

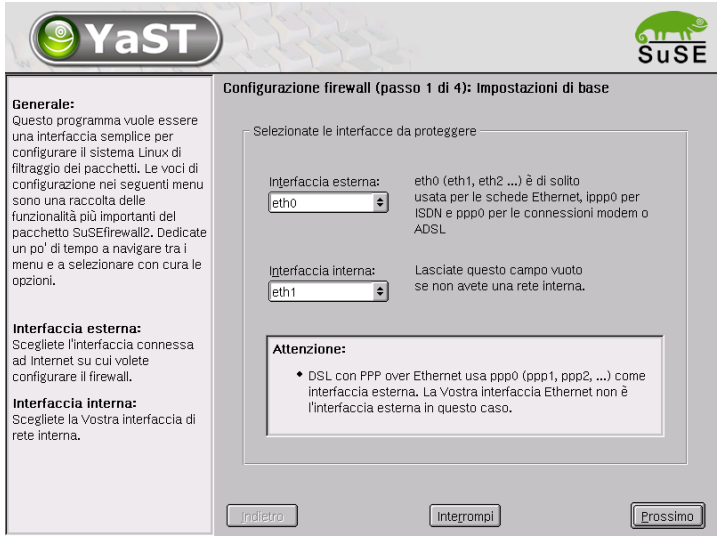


Figura 2.7: *SuSE Firewall: Selezionare l' interfaccia*

Sistema

Creare un backup del sistema

Il modulo backup di YaST2 vi permette di fare un backup del vostro sistema. Comunque il backup creato con questo modulo non include tutto il sistema, ma salva solo le informazioni sui pacchetti modificati, di aree di archiviazione cruciali e file di configurazione.

Durante il processo configurativo potete determinare di quali file eseguire un backup. Di default, si effettua un copia di sicurezza delle informazioni su ogni pacchetto modificato dall'ultima installazione. Inoltre possono essere inclusi dati che non appartengono ai pacchetti, come è il caso di tanti file di configurazione sotto `/etc` o nelle directory sotto `/home`. E infine il backup può includere aree di archiviazione cruciali dell'hard disk di fondamentale importanza al momento del ripristino di un sistema, cosa che rigurda in particolar modo la tabella delle partizioni o il master boot record (MBR).

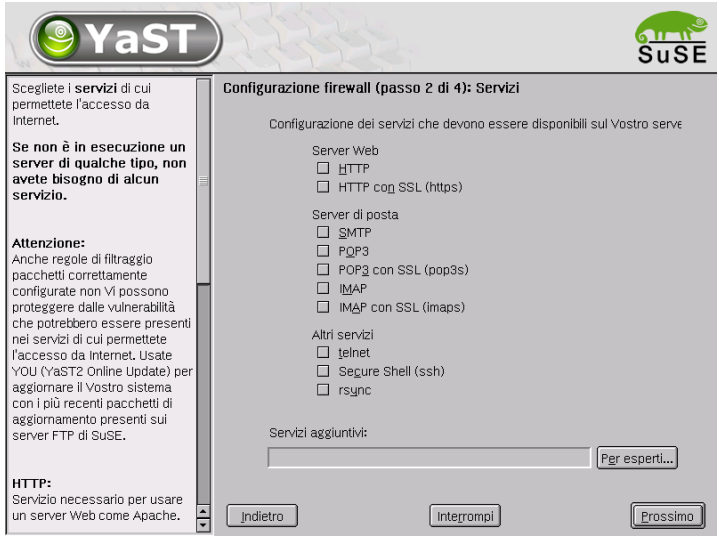


Figura 2.8: *SuSE Firewall: Servizi accessibili dall'esterno*

Ripristina sistema

Qui (vedi figura 2.9 nella pagina seguente) potete ripristinare il vostro sistema dall'archivio backup. Seguite le istruzioni in YaST2. Premete su 'Prossimo' per passare da un dialogo all'altro. Innanzitutto dovete specificare la locazione dell'archivio (dispositivo rimovibile, file locale oppure rete (NFS)). Continuando, viene mostrata una descrizione dei contenuti dei singoli archivi, così da poter decidere cosa ripristinare dall'archivio.

Inoltre vi sono due dialoghi per deinstallare dei pacchetti che si sono aggiunti dall'ultimo backup e reistallare pacchetti eliminati all'ultimo backup. Così avete la possibilità di riportare il vostro sistema esattamente nello stato dell'ultimo backup.

Attenzione

Dato che con questo modulo potete installare, sostituire o deinstallare numerosi pacchetti e file, usatelo solo se avete già una certa dimestichezza nell'eseguire dei backup, altrimenti potreste perdere i vostri dati.

Attenzione

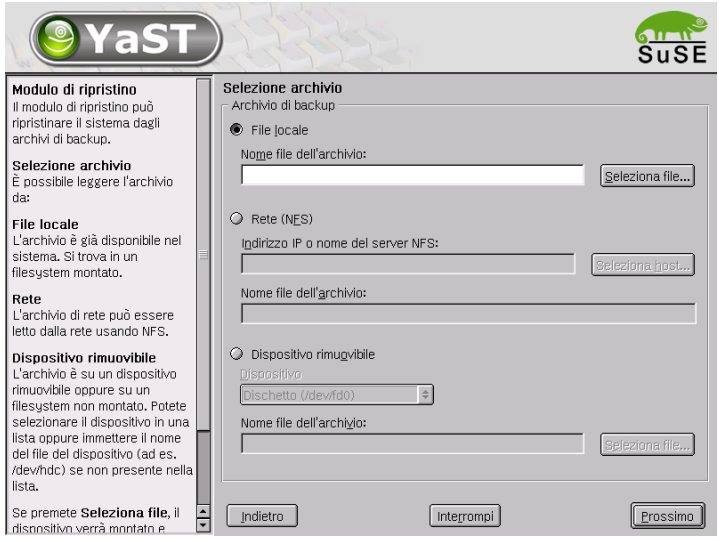


Figura 2.9: *Schermata iniziale del modulo di ripristino*

Editor per sysconfig

La directory `/etc/sysconfig` contiene i file con le impostazioni principali per SuSE Linux Enterprise Server che prima venivano amministrate centralmente nel file `/etc/rc.config`. L'editor per sysconfig mostra le impostazioni possibili in modo chiaro. I valori si lasciano modificare e salvare nei singoli file di configurazione.

La sezione *SuSEconfig, /etc/sysconfig e /etc/rc.config* a pagina 167 ss contiene informazioni dettagliate sull'editor per sysconfig e variabili sysconfig,

Editor dei runlevel

Il runlevel del sistema, il suo "modo operativo" viene avviato dopo il boot del sistema. Su SuSE Linux Enterprise Server, si tratta normalmente del runlevel 5 (sistema multiutente completo con rete e XDM, il login grafico). Con questo modulo potete modificare il runlevel predefinito e indicare il runlevel in cui eseguire il servizio. Vedi tabella 8.1 a pagina 161. I runlevel sotto Linux sono descritti dettagliatamente nella sezione *I runlevel* a pagina 160.

Partizionatore

Con questo tool di partizionamento potete elaborare, cancellare le partizioni esistenti o creare di nuove. Da qui giungete alla configurazione di Soft-RAID e LVM .

Nota

Tante utili indicazioni riguardanti il partizionamento si trovano nel manuale di SuSE Linux Enterprise Server di *Installazione*.

Nota

Di solito le partizioni vengono stabilite durante l'installazione. Se, tuttavia, per motivi di spazio, avete bisogno di un secondo disco rigido, potrete integrarlo nel sistema Linux esistente. Per far ciò, partizionate il nuovo disco rigido, montatelo e registratelo nel file `/etc/fstab`. Potrebbe anche rendersi necessario spostare alcuni dati per trasferire una partizione `/opt` troppo piccola sul nuovo disco rigido.

Nel caso in cui vogliate cambiare le partizioni di un disco rigido su cui state lavorando, dovrete fare molta attenzione: è possibile, ma dovrete riavviare il sistema subito dopo. E' più sicuro ripartizionare il disco rigido dopo averne fatto il boot dal CD. Il bottone 'Esperti...' visualizza un menù a popup con i seguenti comandi:

Rileggi tabella di partizione Per rileggere le partizioni del vostro disco rigido. Questo comando vi serve, ad esempio, ogni volta che abbiate partizionato il disco manualmente, dalla console di testo.

Usa punti di mount del /etc/fstab esistente Ciò è rilevante solo durante l'installazione. Far leggere il vecchio `fstab` è utile per reinstallare completamente il vostro sistema invece di cercare di eseguire degli adattamenti. In questo caso non è necessario inserire manualmente i punti di mount.

Cancella tabella di partizione e disk label Con questo comando, potrete sovrapporre completamente la nuova tabella delle partizioni alla vecchia. Vi servirà nel caso in cui, ad esempio abbiate problemi con label non ordinarie. Con questo metodo, tuttavia, perderete tutti i dati del disco rigido.

Logical Volume Manager (LVM)

Il Logical Volume Manager (LVM) vi permette di ripartire in modo flessibile lo spazio del vostro disco rigido in diversi filesystem. Dal momento che la

modifica delle partizioni in un sistema in uso può diventare molto complicata, si è pensato di creare l'LVM: esso mette a disposizione un "pool" virtuale (Volume Group ovvero VG) di memoria, dal quale, in caso di necessità, possano essere creati dei volumi logici (LV). Il sistema operativo potrà poi ricorrere a questi ultimi, anzicché alle partizioni fisiche.

Particolarità:

- Potete riunire più dischi rigidi/partizioni in un'unica grande partizione logica.
- Se un LV si riempie (per esempio `/usr`), potete espanderlo, in presenza della configurazione adeguata.
- Con l'LVM, potrete espandere dischi rigidi o LV addirittura a sistema caldo, a condizione che disponiate di hardware "Hot-Swapable", l'unico adatto a questo tipo di operazione.

Implementare LVM si rivela essere utile già per PC domestici usati intensamente o piccoli server. Se la mole dei vostri dati cresce continuamente, come nel caso di banche dati, archivi MP3 o directory di utenti, il Logical Volume Manager fa per voi. Esso vi permette di avere file di sistema più grandi di un hard disk. Un ulteriore vantaggio del LVM è che si possono aggiungere fino a 256 LV. Tenete presente che lavorare con LVM differisce considerevolmente rispetto all'impiego di partizioni.

Nell'appendice del manuale di *Installazione* di SuSE Linux Enterprise Server trovate una guida dettagliata in tema di configurazione di LVM.

Per maggiori informazioni ed un'introduzione alla configurazione del "Logical Volume Manager" (LVM), consultate l'Howto su LVM ufficiale o un documento SuSE:

- `http://www.sistina.com/lvm/Pages/howto.html`
- `http://www.suse.com/us/support/oracle/`

Soft-RAID

RAID (ingl. *Redundant Array of Inexpensive Disks*) serve ad unificare più partizioni in un unico grande disco rigido "virtuale", con lo scopo di ottimizzare le prestazioni del sistema e la sicurezza dei dati. Tuttavia, l'uno si realizza a spese dell'altro. Il cosiddetto "RAID-Level" definisce la fusione e la gestione comune dei dischi rigidi eseguita da un controllore RAID.

Al posto di un controllore RAID, che per qualcuno potrebbe risultare troppo costoso, si può ricorrere anche ad un Soft-RAID. SuSE Linux Enterprise Server vi offre la possibilità di unificare, con YaST2, dischi diversi in un unico sistema Soft-RAID, un'alternativa più economica dell'hardware RAID.

Livelli di RAID diffusi

RAID 0 Questo livello migliora l' accesso ai dati. In linea di principio, non si tratta di un vero e proprio RAID, dal momento che non offre il salvataggio dei dati, ma si usa ormai definirlo così. In un sistema "RAID 0", si uniscono almeno due dischi rigidi. La prestazione è molto buona, con un unico difetto: se anche uno solo dei vostri dischi rigidi dovesse venire a mancare, il sistema RAID sarà distrutto e i vostri dati andranno persi.

RAID 1 Questo livello vi offre una sicurezza estremamente soddisfacente, dal momento che i vostri dati vengono copiati in rapporto di 1:1 su di un altro disco rigido. Questo procedimento viene definito "specchiamento dei dischi rigidi": se uno dei dischi viene danneggiato, disporrete di una copia esatta del suo contenuto su un altro disco. Teoricamente, potreste perdere tutti dischi tranne uno senza dover rinunciare ai vostri dati. Con un RAID 1 (più lento del 10-20 %), la prestazione di scrittura risente dello specchiamento. In compenso, la lettura è molto più veloce rispetto ad un unico disco rigido fisico, perché i dati sono doppiati e quindi leggibili parallelamente.

RAID 5 RAID 5 rappresenta un compromesso ottimizzato tra i due level precedenti, per quel che riguarda prestazione e ridondanza. Il potenziale del disco rigido corrisponde al numero dei dischi impiegati meno uno. I dati vengono distribuiti tra i dischi come con RAID 0. Alla sicurezza ci pensano i "blocchi di parità", che, con RAID 5, vengono costruiti su una delle partizioni e collegati con XOR l'uno all'altro: in questo modo, in caso di perdita di una partizione, è possibile ricostruirne il contenuto secondo XOR, tramite il corrispondente blocco di parità. Tuttavia, nel caso di RAID 5, bisogna assolutamente impedire che venga danneggiato più di un disco alla volta: se uno viene distrutto, deve essere immediatamente sostituito, affinché non ne vadano persi anche i dati.

Istruzioni per la configurazione e maggiori dettagli su Soft RAID sono reperibili nei HOWTO all'indirizzo:

- `/usr/share/doc/packages/raidtools/Software-RAID-HOWTO.html`

- http://www.LinuxDoc.org/HOWTO/Software-RAID-HOWTO.html

oppure tramite una mailing list Linux RAID, come:

- http://www.mail-archive.com/linux-raid@vger.rutgers.edu .

Selezionate il fuso orario

Il fuso orario lo avete settato già durante il processo di installazione e qui avete la possibilità di modificarlo. Fate clic sul vostro paese nella lista e selezionate 'Ora locale' o 'GMT' (Greenwich Mean Time). 'GMT' viene spesso usato su sistemi Linux. I computer con sistemi operativi aggiuntivi, come Windows, spesso usano l'ora locale.

Selezione della lingua

Qui impostate la lingua per il vostro sistema Linux. La lingua può essere sostituita in ogni momento. La lingua selezionata in YaST2 viene applicata all'intero sistema.

Misc

Log di avvio

Il protocollo di avvio contiene i messaggi delle schermate che vengono visualizzate durante l'avvio del computer. Il protocollo di avvio viene archiviato sotto `/var/log/boot.msg`. Usate questo modulo YaST2 per prendere visione del protocollo, per esempio, per controllare se tutti i servizi e funzioni sono state avviate come previsto.

Log di sistema

Tutte le operazioni del vostro computer vengono protocollati sotto `/var/log/messsages`. Qui trovate anche i messaggi del Kernel, disposti secondo la data e l'ora.

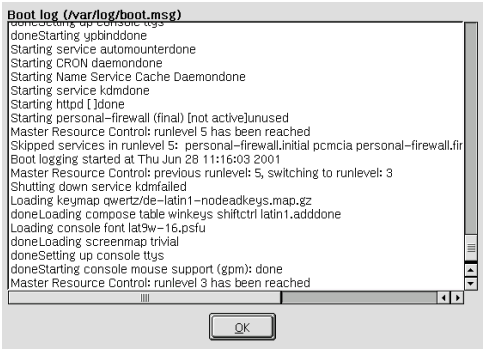


Figura 2.10: *Visualizzare il log di avvio*

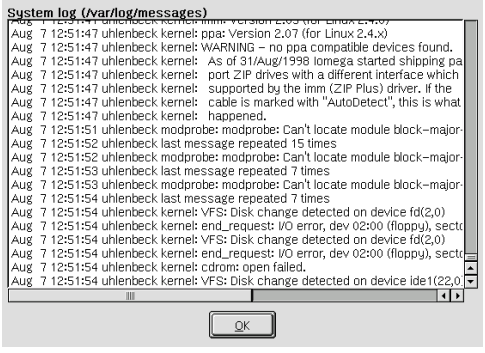


Figura 2.11: *Display System Protocol*

Carica il CD dei driver del produttore

Qui potete installare automaticamente i driver di dispositivi da un CD dei driver Linux che contiene i driver per SuSE Linux Enterprise Server. Se installate SuSE Linux Enterprise Server per la prima volta, con questo modulo di YaST2 potrete caricare i driver necessari dal CD del produttore dopo l'installazione.

Il sistema X Window

Un pò di storia

De facto l'X Window System rappresenta l'interfaccia grafica per UNIX. Comunque l'X Window System va anche oltre a questo — X11 è un sistema basato sulla rete. Applicazioni che girano sul computer `terra` possono visualizzare l'output su `sole`, ammesso i due computer siano connessi in una rete. Questa rete può essere una rete di tipo locale (LAN) oppure si può trattare anche di una connessione tramite Internet di due computer distanti migliaia di chilometri l'uno dall'altro.

X11 è una sfida che è stata raccolta dalla DEC (Digital Equipment Corporation) e del progetto Athena presso il MIT (Massachusetts Institute of Technology). Nel settembre del 1987 esce la prima release di X11R1. A partire dalla release 6 è l' X Consortium, Inc. ad essere responsabile dello sviluppo dell'X Window System.

XFree86 ™ è un'implementazione libera di X server per PC. E' stata sviluppata da pochi sviluppatori ambizionati che nel 1992 hanno fondato il team XFree86. Nel 1994, questo team fondò The XFree86 Project con l'obiettivo di continuare a sviluppare l'X11 e di metterlo a disposizione di tutti. Dal marzo del 2000 si può scaricare dal sito `http://www.XFree86.org` la major release di XFree86-4.0 completamente rivista. Di default, SuSE Linux Enterprise Server esegue installazione di XFree86-4.0. Più avanti sono riportate le caratteristiche di questa versione.

SuSE ringrazia il team di XFree86 per l'aiuto e per il permesso di includere i server beta sui CD [1].

[1] In parte la presente documentazione è ripresa dal capitolo *Configurare XFree86* da [HHMK96] che Dirk Hohndel ha messo gentilmente a nostra disposizione che è stata di grande aiuto per la stesura della presente documentazione

I seguenti capitoli trattano la configurazione dell'X-server. Tratteremo a riguardo anche SaX2 e xf86config che sono degli strumenti semplici da usare per configurare l'X Window System.

Al contrario dell' xf86config testuale, SaX2 lavora direttamente con l'X server e può venire usato con il mouse.

Attenzione

Siate molto cauti quando configurate il vostro sistema X Window. Non inizializzate il sistema X Window, finché la configurazione non sia terminata. Un sistema configurato in maniera errata può causare danni irreparabili all'hardware (ciò vale soprattutto per monitor a frequenza fissa). Gli autori di questo libro e la SuSE declinano ogni responsabilità per eventuali danni. Non si può però escludere che i metodi qui presentati, che comunque sono stati sottoposte a delle verifiche esaustive, non causino alcun danno al vostro hardware.

Attenzione

La versione 4.x di XFree86

Questa versione di SuSE Linux Enterprise Server contiene l'attuale versione 4.x di XFree86 che si differenzia in diversi punti dalla versione 3.3 finora inclusa. Nell'uso della superficie grafica ci sono per l'utente solo poche differenze, anche le applicazioni come per esempio il desktop grafico di KDE o GNOME continuano a comportarsi come nella versione 3.3.6 inclusa nelle distribuzioni precedenti.

I vantaggi della nuova versione

Il nuovo X-server non è più un programma monolitico, bensì solo una struttura di base relativamente piccola in cui possono venire aggiunti in seguito all' occorrenza i necessari moduli di programma. Per esempio non ci più differenti X server per differenti schede grafiche come nelle versioni precedenti, bensì solo un programma eseguibile chiamato XFree86 che trovate nella directory `/usr/X11R6/bin` e che è inoltre anche l'X server attuale. Il driver grafico che controlla le schede grafiche è un modolo caricabile.

Si procede in modo simile anche per il supporto di diversi dispositivi di input, fonts o protocolli X; anche in questo caso si tratta di singoli moduli che possono essere caricati in un secondo momento dall'X server. Di solito non

serve che interveniate. La configurazione dei moduli necessari al funzionamento della superficie grafica del vostro computer, viene svolta, per quanto possibile, da SaX2.

Grazie al concetto dei moduli, è molto semplice per il produttore, implementare un driver per hardware un pò fuori dal comune come schermi tattili o nuove schede grafiche. Gli sviluppatori hanno persino provveduto affinchè i moduli necessari per i diversi sistemi operativi possano venire messi a disposizione solo una volta; ciò significa che un modulo del driver grafico compilato per esempio sotto FreeBSD, può anche venire usato sotto Linux e viceversa. Questa portabilità è però limitata ad una sola piattaforma hardware; un modulo Linux compilato per i PowerPC non può venire utilizzato su un PC Intel.

Inoltre il supporto del mouse è stato migliorato significativamente. Soprattutto, sotto sforzo i tempi di reazione del mouse ai movimenti è considerevolmente migliorato rispetto alla precedente versione di X server XFree86. In generale è migliorata la rapidità dell'output, in genere le operazioni grafiche vengono eseguite più velocemente rispetto al vecchio X-server (fatto dovuto alla rielaborata XAA (*XFree86 Acceleration Architecture*).

Rispetto a XFree86 3.3.x, il file di configurazione ha un formato un po' diverso e risiede ora sotto `/etc/X11/XF86Config`. Se volete eseguire un "fine tuning" (una messa a punto finalizzata) del vostro X server, o se volete effettuare configurazioni speciali, troverete informazioni dettagliate nella sezione *Come ottimizzare l'installazione del sistema X Window* a pagina 43.

Inoltre è stato migliorato il logging di errori. L'X server genera un file protocollo molto dettagliato che troverete dopo ogni avvio dell'X server nel file `/var/log/XFree86.0.log`. Fra le caratteristiche della nuova versione vi è anche il supporto di opzioni speciali come True-Type-Fonts e la correzione gamma.

Configurazione con SaX2

Essa viene normalmente configurata già durante l'installazione. Per modificarne i valori o eseguire operazioni come l'allaccio di un altro monitor a sistema caldo, potrete tuttavia ricorrere a SaX2. Prima di ogni modifica, viene salvata la configurazione attuale.

Dopodiché, il programma vi porta nel medesimo dialogo dell'installazione di SuSE Linux Enterprise Server.

Avete ora la scelta tra 'Solo testo' e la superficie grafica. Per quest'ultima, vi vengono mostrati i valori in uso: la risoluzione dello schermo, la profondità

cromatica, la frequenza di ripetizione delle immagini, il produttore ed il tipo del monitor, se il programma ha potuto riconoscerlo automaticamente. Se state appena installando il sistema o una nuova scheda grafica, apparirà un'altra piccola finestra, nella quale vi si chiede se desideriate attivare l'accelerazione tridimensionale per la vostra scheda grafica.

Cliccate su 'Modifica': verrà avviato SaX2, lo strumento di configurazione dei dispositivi di immissione e visualizzazione, in una finestra a parte (fig. *Configurazione con SaX2*).

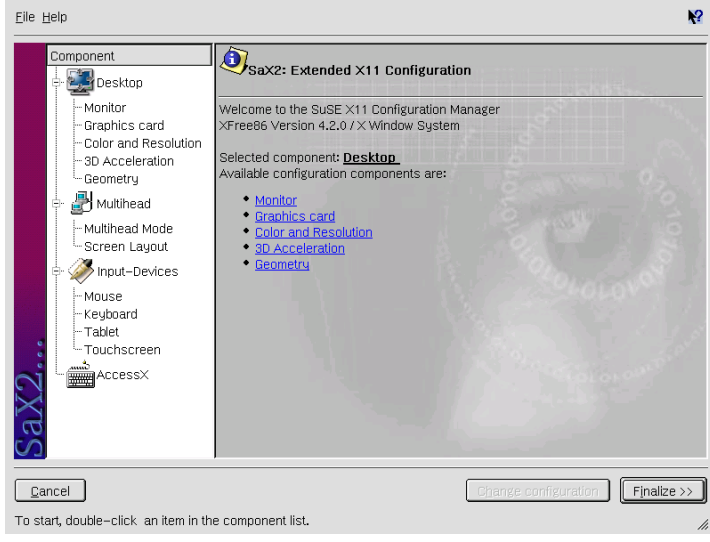


Figura 3.1: *La nuova finestra principale di SaX2*

SaX2: la finestra principale

Nella barra di navigazione a sinistra, vedete quattro punti principali: 'Display', 'Dispositivi di immissione', 'Multihead' e 'AccessX'. 'Display' è la sezione dedicata all'impostazione dello schermo, della scheda grafica, della profondità cromatica, della risoluzione, posizione e dimensione della videata. Alla voce 'Dispositivi di immissione', potete configurare tastiera e mouse, nonché, se necessario, un touchscreen ed una tavola grafica. Nel menù 'Multihead', invece, potete impostare un sistema a più schermi (vd. *Multihead* a pagina 40), assieme al modo della rappresentazione multihead e la disposizione degli schermi sulla vostra scrivania. 'AccessX' è uno strumento utilissimo,

che serve a muovere il puntatore del mouse con la tastierina numerica, nel caso in cui vi troviate a caricare un sistema senza mouse o il mouse ancora non funzioni. Potete anche qui fissare la velocità del puntatore quando esso venga guidato dalla tastierina.

Nel dialogo dedicato allo schermo e scheda grafica, impostate i relativi modelli. Normalmente, questi vengono riconosciuti automaticamente dal sistema, nel qual caso vi potrete risparmiare la fatica.
Qualora il vostro monitor non dovesse venir riconosciuto automaticamente, il programma vi porta in un dialogo di selezione del modello. Questo dialogo vi offre una lista completa delle case produttrici e modelli. Se non trovate il vostro, copiate manualmente i valori dalla documentazione del vostro monitor o selezionate i parametri preimpostati, i cosiddetti modi Vesa.

Alla fine delle vostre impostazioni riguardanti il monitor e scheda grafica, cliccando su 'Chiudi' nella finestra principale, vi sarà offerta la possibilità di testare la vostra configurazione. In questo modo potrete verificare che la configurazione sia stata accettata dai dispositivi. Se, durante il test, l'immagine del monitor dovesse essere disturbata, interrompete il test con il tasto Esc e riducete i valori della frequenza di ripetizione, della definizione o della profondità cromatica. Tutte le vostre modifiche, indipendentemente dal test, diventano comunque valide dopo aver riavviato il sistema grafico, vale a dire l'X-Server. Se state usando KDE, basta uscire e rifare il login.

Display

Cliccate su 'Modifica configurazione' → 'Proprietà' ed apparirà una finestra con le tre guide 'Monitor', 'Frequenze' ed 'Ampliato':

- 'Monitor': nella parte sinistra della finestra, scegliete il produttore e, a destra, il modello. Se siete in possesso di dischetti con unità di disco per Linux, inseriteli e cliccate su 'Dischetto unità disco'.
- 'Frequenze': configurate le frequenze orizzontali e verticali del vostro schermo. La frequenza verticale non è altro che la frequenza di ripetizione dell'immagine. Normalmente, il programma sonderà i valori massimi e minimi del modello e ve li mostrerà in questo dialogo. Di regola, non saranno necessarie modifiche.
- 'Avanzato': impostate qui ancora un paio di opzioni per il vostro schermo. Nell'area di selezione in alto, potete impostare il metodo di calcolo della definizione e della geometria del monitor. Modificate i valori preimpostati solo se questi sono sbagliati e, se nel test, non riuscite ad ottenere un'immagine stabile. Potete anche impostare le dimensioni della videata ed il modo di risparmio energetico "DPMS".

Scheda grafica

Nel dialogo della scheda grafica, vedrete due guide: 'Generale' ed 'Avanzato':

- 'Generale': come per il monitor, inserite qui la marca (a sinistra) ed il modello (a destra) della vostra scheda grafica.
- 'Avanzato': a destra, determinate se il vostro schermo debba essere ruotato verso sinistra o perpendicolarmente (come nel caso di alcuni schermi TFT). I valori di BusID possono restare così come sono, dal momento che servono solo in sistemi multischermo. Non modificate neanche le opzioni delle schede, specialmente se non ve ne intendete e non sapete cosa significhino. In caso di necessità, vi preghiamo di leggere attentamente la documentazione della vostra scheda.

Nota

La configurazione di schede grafiche supportate solo da XFree86 3.3.6 non fa più parte dell'installazione da SuSE Linux Enterprise Server 8.1. Un esempio tipico sono i modelli più vecchi di schede S3 PCI. YaST2 configura, invece, il framebuffer non accelerato ovvero il driver vga generico a 16 colori per questo tipo di schede, a seconda del modello. Se il problema vi riguarda, configurate XFree86 3.3.6 separatamente, con l'aiuto di SaX 1, digitando il comando `sax` nella riga di comando.

Nota

Colori/Definizione/i)

Anche qui, troverete tre guide: 'Colori', 'Definizione' e 'Avanzato'.

- 'Colori': indipendentemente dall'hardware, potete scegliere tra i valori 16, 256, 32768, 65536 e 16,7 milioni di colori per 4, 8, 15, 16 o 24 bit. Per una buona immagine, vi consigliamo di non scegliere meno di 256 colori.
- 'Risoluzione': questo valore viene identificato durante l'installazione ed il programma vi proporrà delle combinazioni di risoluzione e profondità cromatica che possano essere visualizzati dal vostro hardware senza errori. Pertanto, nelle nuove versioni di SuSE Linux Enterprise Server, non si corre quasi alcun pericolo di danneggiare l'hardware con impostazioni sbagliate. Se, tuttavia, avete intenzione di cambiare

la risoluzione manualmente, vi preghiamo di leggere attentamente la documentazione del vostro hardware e di assicurarvi che i nuovi valori possano essere visualizzati dall'hardware.

- 'Avanzato': potete qui aggiungere dei valori personali di risoluzione, i quali verranno poi aggiunti alla selezione generale.

Accelerazione tridimensionale

Se, durante l'installazione del sistema o di una scheda grafica nuova, non avete attivato l'accelerazione tridimensionale della scheda, potete farlo adesso, in questa finestra.

Posizione e dimensioni dello schermo

In entrambe le schede, potete calibrare la posizione e le dimensioni della videata con i tasti freccia (cfr. fig. 3.2). Se avete un ambiente multihead (più di uno schermo), potete passare da un monitor all'altro con il pulsante 'Schermo successivo', per impostare dimensioni e posizione di tutti gli schermi. Salvate la configurazione con 'Salva'.

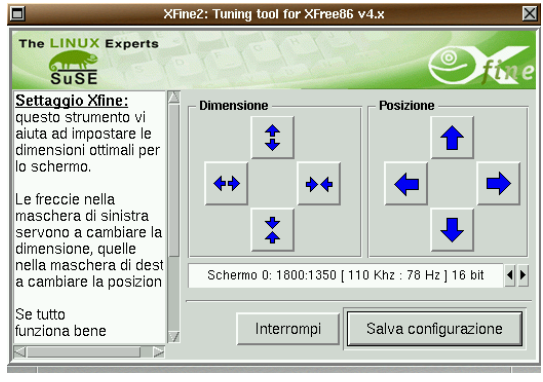


Figura 3.2: *Modifica della geometria dello schermo*

Attenzione

Anche se vi sono dei meccanismi di protezione, siate particolarmente cauti nel configurare le frequenze. I valori sbagliati potrebbero distruggere lo schermo. Consultate il manuale del vostro monitor.

Attenzione

Multihead

Se, nel vostro pc, vi è più di una scheda grafica o una scheda con più uscite, potete allacciare più schermi al vostro sistema. Con due schermi, avrete un sistema dualhead, mentre, con più di due, si tratta di un multihead. SaX2 riconosce automaticamente la presenza di più schede e vi adatta la configurazione. Nel dialogo multihead di SaX, potete fissare il modo multihead e la disposizione degli schermi. Potete scegliere tra tre modi: 'Tradizionale' (default), 'Xinerama' e 'Cloned':

- 'Multihead tradizionale': ogni monitor è un'unità a sé stante. Solo il mouse si può muovere da uno schermo all'altro.
- 'Cloned Multihead': si usa soprattutto in presentazioni o per grandi muri di schermi. Ogni monitor ha lo stesso contenuto ed il mouse non può uscire dallo schermo principale.
- 'Xinerama Multihead': Tutti gli schermi vengono fusi in uno, il che vuol dire che le finestre dei programmi possono essere posizionati su uno schermo qualsiasi o ingrandite fino a coprire tutti i monitor.

Il layout di un ambiente multihead è la disposizione degli schermi ed i rapporti tra uno schermo e l'altro. SaX2 assegna un layout standard nella sequenza delle schede grafiche riconosciute. Con questo formato, tutti gli schermi risultano allineati da sinistra a destra. Nel dialogo 'Layout' dello strumento di configurazione del multihead, impostate l'ordine dei monitor sulla vostra scrivania, spostando con il mouse i simboli degli schermi lungo la griglia.

Chiudete il dialogo di Layout e testate la configurazione degli schermi cliccando sul pulsante 'Test'.

Vi preghiamo di tenere presente che Linux, al momento, non supporta il 3D in ambiente Xinerama Multihead. In questo caso, pertanto, SaX2 disattiva automaticamente il supporto 3D.

Dispositivi di immissione

Mouse Se il mouse funziona, non avrete bisogno di altre impostazioni. In caso contrario, usate la tastierina numerica come descritto nella sezione *AccessX* a pagina 42.

Se non dovesse funzionare il riconoscimento automatico, configurate il vostro mouse manualmente. Troverete la descrizione del tipo di mouse nella sua documentazione.

Selezionatela dalla lista dei tipi di mouse supportati. Selezionate il tipo di mouse e confermate con un clic del tasto (5) della tastierina numerica.

Tastiera In questo dialogo, impostate il tipo di tastiera nel campo di selezione in alto. Scegliete anche la lingua della tastiera (ovvero la disposizione dei tasti in uso nel vostro paese). Testate poi il funzionamento della configurazione, digitando dei caratteri speciali, come "à" o "é".

Lasciate la casella di attivazione delle vocali accentate come preimpostata per la vostra lingua. Salvate la configurazione con 'Fine'.

Touchscreen Linux supporta, al momento, i touchscreen XFree86 della Microtouch e della Elographics. SaX2 riconosce automaticamente solo il monitor, ma non il toucher, che va visto a sua volta come un dispositivo di immissione. Procedete quindi come segue, per configurare il toucher:

1. Avviate SaX2 e passate a 'Dispositivi di immissione' → 'Touchscreen'.
2. Cliccate su 'Aggiungi' ed aggiungete un touchscreen.
3. Salvate la configurazione con un clic su 'Fine'. Non è necessario testare la configurazione.

I touchscreen sono molto versatili e, nella maggior parte dei casi, devono essere prima calibrati. Linux, purtroppo, ancora non vi può offrire alcuno strumento di calibrazione dei touchscreen. La configurazione standard include buoni parametri di default per i rapporti dimensionali dei touchscreen, di modo che non sono normalmente necessarie altre impostazioni a questo riguardo.

Tavola grafica XFree86 supporta ancora poche tavole grafiche. SaX2 vi offre la configurazione tramite USB o interfaccia seriale. Dal punto di vista della configurazione, una tavola grafica equivale ad un mouse, ovvero, più in generale, ad un dispositivo di immissione. Vi consigliamo di procedere come segue:

1. Avviate SaX2 e passate a 'Dispositivi di immissione' → 'Tavola grafica'.
2. Cliccate 'Aggiungi', selezionate nel dialogo che appare la marca e aggiungete una tavola grafica dalla lista che vi viene mostrata.

3. Eventualmente, selezionate, nelle caselle a destra, l'allaccio di un'altra matita o gomma da cancellare.
4. Se avete una tavola seriale, verificate che l'allaccio sia quello giusto per tutti gli accessori: `/dev/ttyS0` è la prima interfaccia seriale, `/dev/ttyS1` la seconda e via di seguito.
5. Salvate la configurazione, cliccando su 'Fine'.

AccessX

Se il vostro pc non ha mouse ed attivate AccessX dopo aver avviato SaX2, potrete guidare come segue il puntatore del mouse sul vostro schermo con la tastierina numerica:

- **Button 1** corrisponde al tasto (%)
  Questo tasto attiva il tasto sinistro del mouse
- **Button 2** corrisponde al tasto (X)
  Questo tasto attiva il tasto di mezzo del mouse
- **Button 3** corrisponde al tasto (-)
  Questo tasto attiva il tasto destro del mouse
- **Click** corrisponde al tasto (5)
  Questo tasto clicca sul button previamente attivato. Se non avete attivato alcun button, si usa il tasto sinistro del mouse. L'attivazione dei tasti, dopo il clic, viene riportata all'impostazione di default.
- **Double Click** corrisponde al tasto (+)
  Questo tasto funziona come il (5), con la differenza che esso genera un doppio clic.
- **Button Lock** corrisponde al tasto (0)
  Questo tasto funziona come il (5) con la differenza che genera solo una pressione del button e la mantiene.
- **Button Release** corrisponde al tasto (Canc)
  Questo tasto rilascia il button che era rimasto premuto con lo (0).
- **Freccia in alto a sinistra** corrisponde al tasto (7)
  Questo tasto muove il mouse in alto a sinistra.
- **Freccia verso l'alto** corrisponde al tasto (8)
  Questo tasto muove il mouse verso l'alto.

- **Freccia in alto a destra** corrisponde al tasto ⑨
  Questo tasto muove il mouse in alto a destra.
- **Freccia verso sinistra** corrisponde al tasto ④
  Questo tasto muove il mouse verso sinistra.
- **Freccia verso destra** corrisponde al tasto ⑥
  Questo tasto muove il mouse verso destra.
- **Freccia in basso a sinistra** corrisponde al tasto ①
  Questo tasto muove il mouse in basso a sinistra.
- **Freccia verso il basso** corrisponde al tasto ②
  Questo tasto muove il mouse verso il basso.
- **Freccia in basso a destra** corrisponde al tasto ③
  Questo tasto muove il mouse in basso a destra.

La velocità di reazione del puntatore al tasto va impostata con la levetta apposita.

Come ottimizzare l'installazione del sistema X Window

In questo capitolo descriveremo la struttura del file di configurazione `/etc/X11/XF86Config`. Questo file è suddiviso in sezioni (ingl. *sections*), introdotte dalla parola chiave Section "identificatore", e che terminano con EndSection. Ci limiteremo a presentare le sezioni principali.

Alla fine imparerete come integrare ulteriori font, come configurare gli input device di registrazione e come viene realizzato l'acceleramento 3D. Questo viene naturalmente eseguito anche in determinate sezioni del file `XF86Config`, ma l'integrazione di un ulteriore font richiede l'aiuto di programmi esterni che però vengono forniti con SuSE Linux Enterprise Server o fanno parte dell'installazione di default. I procedimenti qui accennati vogliono solo chiarire le possibilità esistenti e servire da stimolo, e non hanno certamente la pretesa di essere completi.

I programmi SaX2 e xf86config (per XFree86 4.x) creano il file `XF86 Config` in `/etc/X11`. Questo è il file primario di configurazione per l' X Window System. Qui si trovano le indicazioni su mouse, monitor e scheda grafica.

`XF86Config` è formato da più Sections, ognuna delle quali si occupa di un aspetto della configurazione. Una sezione ha sempre la forma seguente:

```
Section ⟨denominazione della sezione⟩
  registrazione 1
  registrazione 2
 registrazione  n
EndSection
```

Esistono i seguenti tipi di sezioni:

Tipo	**Significato**
Files	Questa sezione descrive i path usati per i font e le tabelle RGB dei colori.
ServerFlags	Qui vengono scelti i server flag.
InputDevice	Tramite questa sezione vengono configurati i device d'ingresso. Contrariamente a XFree86 3.3, vengono configurati tramite questa sezione sia tastiere che mouse come pure speciali input device come touch tables, joysticks etc. Gli indicatori importanti sono qui Driver e le opzioni che stabiliscono Protocol e Device.
Monitor	Descrive il monitor usato. Gli elementi di questa definizione sono: un nome, a cui si rimanda per la definizione degli Screens, la descrizione della banda delle frequenze (Bandwidth) e delle frequenze di sincronizzazione (HorizSync e VertRefresh). Le indicazioni si fanno in MHz, kHz o Hz. Fondamentalmente il server rifiuta ogni modeline che non corrisponda al quelle specifiche del monitor: con questo si evita che, facendo esperimenti con i modeline, possano venire inviate al monitor frequenze troppo alte
Modes	Qui vengono definiti i parametri di raffigurazione delle singole risoluzioni dello schermo. Questi parametri possono venire calcolati da SaX2 in base a valori dati dall'utente e generalmente non devono venire modificati. Potete però eseguire modificazioni manuali se volete per esempio collegare uno schermo di frequenza. Dare qui l'esatta spiegazione dei singoli parametri andrebbe oltre i limiti di questo manuale; troverete però un'accurata definizione dei singoli valori nel file HOWTO `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`.
Device	Questa sezione setta una determinata scheda grafica. Ci si riferisce ad essa con il nome indicato.

Tabella 3.1: *Continua alla pagina seguente...*

Screen	Questa sezione infine racchiude un driver (p.e. vga2 o accel), un monitor e un device; da essa derivano le indicazioni necessarie per XFree86. La sottosezione display permette l'indicazione di risoluzioni virtuali dello schermo (Virtual), del ViewPort e dei modes usati con questo schermo.
ServerLayout	Questa sezione definisce il layout di una configurazione singlehead o multihead. Qui vengono raggruppati in un'unità i device d'immissione InputDevice e gli Screen.

Tabella 3.1: *Sezioni in /etc/X11/XF86Config*

Ora guardiamo da vicino le sezioni Monitor, Device e Screen. Nella pagina di manuale di `manXF86Config` (`man manXF86Config`) si trovano le informazioni sulle altre sezioni.

In `XF86Config` possono trovarsi più sezioni Monitor e Device. Sono possibili anche più sezioni Screen; quale di queste venga usata, dipende dalla sezione successiva ServerLayout.

Screen-Section

Guardiamo per prima la sezione screen; come già accennato, questa raggruppa le sezioni monitor e device e stabilisce quale risoluzione e quale profondità di colori devono essere messe a disposizione.

Una sezione screen può p.e. essere come in 1.

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes       "640x480"
  EndSubSection
  SubSection "Display"
    Depth       8
```

```
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

file 1: *La sezione Screen del file /etc/X11/XF86Config*

La riga Identifier (qui Screen[0]) dà a questa sezione una denominazione univoca, che nella sezione successiva ServerLayout permetterà di riferirsi ad essa in modo univoco.

Le prossime due righe, Device e Monitor, definiscono la scheda grafica e il monitor appartenenti a questa definizione. Questi non sono altro che rimandi, con il relativo nome, alle sezioni device e monitor. Queste sezioni verranno spiegate dettagliatamente più avanti.

Tramite l'indicazione DefaultColorDepth, si può scegliere con quale profondità di colori debba partire il server (se viene inizializzato senza una precisa indicazione della profondità dei colori).

Per ogni profondità di colore segue una sottosezione Display. La profondità di colore per la quale è valida la sottosezione, viene stabilita dalla parola chiave Depth. I valori possibili per Depth sono 8, 15, 16, 24 e 32. Non tutti i moduli dell'X server supportano ognuno dei valori; 24 e 32 bpp hanno la stessa profondità di colori, con la differenza che 24 sceglie il modo 24 bpp packed-pixel e 32 il modo 24 bpp padded-pixel.

Dopo la profondità di colore, con Modes viene stabilito un elenco di risoluzioni. Questo elenco viene letto dall'X-server da sinistra a destra. Per ogni risoluzione, viene cercata, nella sezione monitor, una Modeline adatta che possa venire visualizzata dallo schermo e dalla scheda grafica.

La prima risoluzione, in questo senso, è quella con la quale parte l'X-server (il cosiddetto Default-Mode). Con i tasti Ctrl +Alt +Grigio + si può navigare a destra, con i tasti Ctrl +Alt +Grigio − si può navigare a sinistra. In questo modo si può variare la risoluzione dello schermo mentre si sta lavorando col sistema X-Window.

L'ultima riga della sottosezione Display con Depth 16 si riferisce alla dimensione dello schermo virtuale. La dimensione massima dello schermo virtuale dipende dalla quantità di memoria della scheda video e dalla profondità di colore desiderata, e non dalla risoluzione massima del monitor. Dato che le recenti schede grafiche offrono tanta memoria grafica, possono generare desktop virtuali di dimensione notevole. Tenete presente però che non potrete più

utilizzare le funzionalità tridimensionali, se in pratica avete riempito l'intera memoria grafica con un desktop virtuale. Se p.e. la scheda video ha 1 MB di RAM , lo schermo virtuale - con 8 Bit di profondità di colore- può arrivare fino a 4096x4096(!) Pixel. Specialmente con server accelerati non è consigliabile usare per lo schermo virtuale l'intera memoria della scheda video, poiché la memoria che resta libera viene utilizzata da questo server per diverse font e graphic-cache.

Device-Section

Una device section descrive una determinata scheda grafica.
Nell'`XF86Config` possono essere contenute molte device section, sempre che il loro nome, indicato con la parola chiave Identifier, sia sempre diverso. In genere – se usate più di una scheda grafica – le sezioni vengono numerate, la prima con Device[0], la seconda con Device[1] etc. Nel seguente file potete vedere la parte della sezione device di un computer con una scheda grafica Matrox Millennium PCI:

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

Se per la configurazione usate SaX2, la device section dovrebbe essere come quella sopra raffigurata. Specialmente Driver e BusID sono dipendenti dall'hardware installato nel vostro computer e vengono automaticamente determinati da SaX2. BusID determina il jumper PCI o AGP in cui è inserita la scheda grafica. Questa concorda con l'ID emesso dal comando lspci. Tenete presente che l'X-server emette le indicazioni in modo decimale, mentre il programma lspci le emette in modo esadecimale!

Tramite il parametro Driver stabilite il driver da usare per questa scheda grafica. I driver vengono cercati dall'X-server nella sottodirectory `driver` tramite ModulePath definito nella sezione Files. Nel caso della Matrox Millennium, il modulo del driver si chiama mga. In una installazione standard, la directory è `/usr/X11R6/lib/modules/drivers`; al nome viene semplicemente "attaccato" `_drv.o`; nel caso del driver mga viene caricato come file driver mga_drv.o.

Tramite ulteriori opzioni, è possibile influenzare il comportamento dell'X-server o del driver. Nella device section, è stata attivata l'opzione sw_cursor.

Questa disattiva l'hardware del cursor del mouse e raffigura il cursor in software. A seconda del modulo del driver, avete a disposizione diverse opzioni, queste si trovano nei file in cui vengono descritti i moduli dei driver, nella directory `/usr/X11R6/lib/X11/doc`. Opzioni valide in generale si trovano nella pagina di manuale di `XF86Config` (`man XF86Config`) e nella pagina di manuale di `XFree86` (`man XFree86`).

Monitor Section e Modes Section

Analogamente alle sezioni device, le sezioni monitor e modes Section, descrivono un monitor. Il file di configurazione `/etc/XF86Config` può contenere un numero qualsiasi di sezioni monitor che devono avere tutte nomi diversi. Nella sezione ServerLayout viene stabilito quale sezione monitor sia rilevante.

Per la definizione del monitor vale, ancor più che per la descrizione della scheda grafica, che la creazione di una monitor section (e specialmente la modes section) venga eseguita da utenti esperti. I componenti principali della modes section sono le modeline in cui vengono indicati il timing orizzontale e verticale per la rispettiva risoluzione. Nella monitor section, vengono registrate le proprietà del monitor e specialmente le frequenze di deflessione.

Attenzione

Senza cognizioni di base sul funzionamento di monitor e scheda grafica, le modeline non dovrebbero venire modificate, poiché ciò potrebbe portare alla distruzione del monitor!

Attenzione

Chi desidera sviluppare una propria descrizione del monitor, dovrebbe prima conoscere la documentazione nella directory `/usr/X11/lib/X11/doc`. In particolar modo da sottolineare [FCR93], in cui vengono dettagliatamente descritte la funzione dell'hardware e la creazione delle modeline.

Fortunatamente, la creazione manuale di modeline o definizioni monitor non sono quasi più necessarie. Se usate un moderno Multisync-Monitor, l'X-server può leggere direttamente dal monitor via DDC le larghezze di banda permesse e la risoluzione ottimale (come già detto in SaX2 nella sezione di configurazione). Se ciò non dovesse essere possibile, potete usare uno dei modi VESA integrato nell'X-server. Questi dovrebbero funzionare perfettamente su tutte le combinazioni di schede grafiche e monitor.

Inserire altri font (TrueType)

Per una normale installazione dell'X-server X11R6 occorre una buona quantità di font che troverete nella directory `/usr/X11R6/lib/X11/fonts` in gruppi logicamente omogenei in sottodirectory. Ricordate che l'X-server considera solo sottodirectory che

- sono registrate come FontPath nella sezione Files nel file `/etc/X11/XF86Config`
- che possiedono un file `fonts.dir` valido
- che non sono state revocate durante il funzionamento dell'X-server con l'aiuto del comando xset −fp
- o sono state inserite durante il funzionamento dell'X-Server con l'aiuto del comando xset +fp

Dalla versione 4.0, XFree86 capisce non soltanto il proprio formato Type1 (un formato PostScript) per font set scalabili e pcf per bitmap font set, ma capisce anche il formato file ttf (ingl. *true type font*). Come già visto nella sezione 1 a pagina 34, questo supporto viene naturalmente realizzato da moduli dell'X-server caricabili. Potete quindi usare con l'X-server anche directory che contengono True-Type-font e non avete praticamente bisogno di alcun lavoro di preparazione.

Un grande vantaggio di quasi tutti i font true-type (oltre alla buona scalabilità), consiste nel fatto che questi font contengono praticamente sempre molto di più dei normali 255 caratteri del font set est europeo codificato in "iso-8859-1". Con questi font set potete rappresentare scritture cirilliche, greche o dell'europa occidentale e con software speciale anche lingue asiatiche. Qui vogliamo descrivere l'uso dei font come font a 8 Bit. Se volete inserire caratteri delle lingue asiatiche, (giapponese, cinese etc.), potete usare editor speciali disponibili anche sotto SuSE Linux Enterprise Server.

Un font a 8 bot comprende 255 caratteri ed estende il font ASCII americano che comprende solo i primi 128 dei 255 possibili caratteri. Un font di testo occupa quindi nella memoria del computer 8 Bit. Poiché 127 caratteri non sono assolutamente sufficienti per contenere tutti i caratteri speciali delle lingue europee, le diverse lingue vengono unite in gruppi che vengono definiti con un breve contrassegno. Il relativo font set viene nominato secondo la relativa norma come font set "iso-8859-x", in cui x è una cifra fra 1 e 15. L'esatta successione dei caratteri nel font set iso-8859-1 o iso-8859-15, potete vederla nella pagina di manuale di `iso-8859-1` (`man iso-8859-1`) o nella pagina di manuale di `iso-8859-15` (`man iso-8859-15`).

Le codificazioni più note si trovano nella tabella 3.2, altre codificazioni potete prenderle dalla suddetta manual page.

Font set	**Regioni supportate, con simboli speciali**
iso-8859-1	Lingue dell'Europa occidentale: spagnolo, tedesco, svedese, danese, ecc.; per il finlandese ed il francese è ormai meglio `iso-8859-15`
iso-8859-2	Europa centro-orientale: ungherese, ceco, rumeno, polacco, tedesco, ecc.
iso-8859-5	Caratteri cirillici per il russo
iso-8859-7	Caratteri grechi per il greco
iso-8859-9	Caratteri per il turco
iso-8859-15	Simile a iso-8859-1, ma con simbolo dell'euro e miglior supporto di finlandese e francese.

Tabella 3.2: *I codici principali*

L'utente deve scegliere la codificazione adatta a seconda della lingua usata. Specialmente nella trasmissione di dati fra diversi computer deve venire trasmessa anche la codificazione. Il vantaggio del procedimento consiste nel fatto che per avere l'appoggio per i caratteri speciali regionali, avete solo bisogno di scegliere la codificazione giusta e subito (quasi) tutti i programmi potranno raffigurare questi caratteri speciali, poiché quasi tutti i programmi usano un valore di 8 bit (un byte) per la rappresentazione di un carattere di testo. Se si seleziona la codificazione sbagliata, anche i caratteri speciali vengono raffigurati in modo errato. Nella maggioranza delle applicazioni X, e anche nel Desktop di KDE, potete scegliere la codificazione del font set, quasi sempre con la configurazione del font set da usare. Nelle applicazioni X, la codificazione viene quasi sempre nominata Encoding.

Lo svantaggio di questa soluzione, è che alcune combinazioni sono semplicemente impossibili: per esempio non è per nulla semplice redigere un testo tedesco con metafonia inserendovi nomi di paesi russi in cirillico.

Questo dilemma può venire risolto con l'uso di Unicode. Unicode non codifica caratteri – diversamente da ASCII – con un Byte, bensì con 2 o più byte cosicchè possono venire raffigurati molti più caratteri. Con l'uso di Unicode potete raffigurare anche le lingue asiatiche con più di 127 caratteri, come il cinese o giapponese o coreano. Lo svantaggio di questa soluzione, è che la maggior parte del software esistente, non è preparato all'uso di questi caratteri ed è possibile leggere o scrivere testi con caratteri Unicode solo con

software speciale. Altre informazioni sull'uso dei font unicode sotto Linux, si trovano sotto http://www.unicode.org. Si parte da presupposto, che in futuro sempre più programmi supportino caratteri Unicode. Sotto SuSE Linux Enterprise Server per digitare testi in Unicode, esiste il programma yudit. Lo trovate nel pacchetto yudit, serie xap o, dopo l'installazione, tramite il menu di SuSE sotto Professionale/Office e lì sotto Editors.

Ed ecco ora passo per passo, la descrizione dell'installazione di font sets supplementari sull'esempio dei font true type.

Trovate prima i font che volete installare nel vostro X Window System. Se sul vostro sistema avete font true type autorizzati, potete usarli. Montate la partizione che contiene questi font.

Se non è ancora esistente, create una directory dei font e andate in questa directory. SuSE Linux Enterprise Server ha già preparato una directory con il nome /usr/X11R6/lib/X11/fonts/truetype; in essa potete copiare i font in oggetto.

```
terra:/root #  cd /usr/X11R6/lib/X11/fonts/truetype
```

Create dei link sui file ttf e sulla directory dei font. Ricordate che per i font true type è necessario anche un programma speciale di nome ttmkfdir, pacchetto ttmkfdir che crea il file fonts.dir. Gli X-font tradizionali vengono integrati solo tramite il comando mkfontdir. Invece di /path/del/fonts inserite il path relativo sotto cui questi font sono disponibili.

```
terra:/usr/X11R6/lib/X11/fonts/truetype #
     ln -s ⟨/pfad/zu/den/fonts⟩/*.ttf .
terra:/usr/X11R6/lib/X11/fonts/truetype #
     /sbin/conf.d/SuSEconfig.fonts
```

Se l' X-Server funziona già, potete rendere disponibili i font in modo dinamico. Digitate:

```
terra:~ #  xset +fp /usr/X11R6/lib/X11/fonts/truetype
```

Suggerimento

Tramite il protocollo X, il comando xset accede all'X-server; devono perciò esistere diritti di accesso sull'X-server corrente, ad esempio, nel caso in cui tux sia l'utente che ha inizializzato l'Xserver. Per ulteriori informazioni, consultare la pagina di manuale di xauth (man xauth).

Suggerimento

Per creare stabilmente dei font, dovreste inserire questo path di ricerca nel file `XF86Config`; per farlo potete usare SaX2. Con 'Aggiungere', aggiungete l'indirizzario nel menù 'Path di ricerca' (alla voce 'Stili' nel dialogo della tastiera) a quelli indicati.

Controllate che i font siano stati configurati giustamente; per farlo usate il comando xlsfonts. Se i set dei caratteri sono installati bene, si ottiene un output di tutti i font installati, incluso i nuovi font true type. Potete anche usare il fontmanager di KDE, che vi fornisce degli esempi di testi con i font installati e si avvia tramite il centro di controllo di KDE.

```
terra:~ #  xlsfonts
```

I font integrati in questo modo possono venire usati per tutte le applicazioni di X.

Stampare

Questo capitolo riassume i principi fondamentali della stampa su Linux. Seguire gli esempi consente di capire i nessi del processo di stampa che a sua volta permetterà di riconoscere e risolvere più celermente dei problemi.

Principi 54
Premesse 57
Configurare la stampante con YaST2 61
Configurazione per applicativi 69
Configurazione manuale di porte di stampanti locali . . . 70
Configurazione manuale di LPRng/lpdfilter 76
Lo spooler di stampante LPRng/lpdfilter 77
Tool di riga di comando per il LPRng 78
Il filtro della stampante del sistema di stampa LPRng/lpdfilter 83
Generare propri filtri di stampante per lo spooler della stampante 92
Il sistema di stampante CUPS 96
Tool della riga di comando per il sistema di stampa CUPS 103
Su Ghostscript 107
a2ps 111
Convertire in PostScript con psutils 113
La codificazione di testi ASCII 119
Stampare nella rete TCP/IP 121

Principi

Con Linux le stampanti vengono indirizzati attraverso cosiddette code di stampa (print queue).

I dati da stampare vengono memorizzati temporaneamente nella queue della stampante da dove lo spooler della stampante li inoltrerà alla stampante.

Spesso i dati da stampare non si trovano nel formato da poter essere inviati direttamente alla stampante. Una grafica per esempio di solito deve essere convertita in un formato che può essere emesso direttamente dalla stampante. Il cosiddetto filtro della stampante si occupa della traduzione dei dati da stampare in un linguaggio compreso dalla stampante.

Suggerimento

Stampare con SuSE Linux Enterprise Server
In questo capitolo tratteremo la configurazione e l'impiego di stampanti su piattaforme SuSE Linux Enterprise Server. Tenete presente che alcune funzionalità (specialmente se dipendono dall'hardware) non sono disponibili sulla vostra piattaforma.

Suggerimento

Esempi per linguaggi di stampante standard

Testo in ASCII La maggior parte delle stampanti emette direttamente almeno testi ASCII. Le stampanti che rappresentano una delle poche eccezioni che non possono stampare direttamente testi in ASCII, vengono indirizzati da uno dei seguenti linguaggi di stampante standard.

PostScript PostScript è il linguaggio standard di Unix/Linux, che permette di stampare direttamente sulle stampanti PostScript. Queste stampanti sono relativamente costose, visto che PostScript è un linguaggio potentissimo ma complesso che richiede dalle stampanti PostScript una laboriosa elaborazione per produrre un copia stampata. Inoltre a causa della licenza si creano dei costi aggiuntivi.

PCL3, PCL4, PCL5e, PCL6, ESC/P , ESC/P2 e ESC/P a matrice Se non vi è una stampante PostScript, il filtro della stampante usa il programma Ghostscript per convertire i dati in uno di questi linguaggi di stampante standard. Viene utilizzato un driver Ghostscript adatto il più possibile al modello della stampante, in modo da considerare le particolarità del modello, per esempio le impostazioni del colore.

Il processo di stampa

1. L'utente o un'applicazione crea un incarico di stampa.
2. I dati da stampare vengono memorizzati temporaneamente nella queue di stampa da dove lo spooler della stampante li inoltra al filtro della stampante.
3. Normalmente il filtro della stampante fa quanto segue:
   (a) Viene determinato il tipo dei dati da stampare.
   (b) Se i dati da stampare non sono di natura PostScript, vengono innanzitutto convertiti nel linguaggio standard PostScript. In particolare testi ASCII vengono convertiti in PostScript con il programma `a2ps`.
   (c) I dati PostScript vengono convertiti eventualmente in un altro linguaggio di stampante.
      - Nel caso di stampanti PostScript, i dati PostScript vengono inviati direttamente alla stampante.
      - Altrimenti il programma Ghostscript viene utilizzato con un driver Ghostscript adatto al relativo modello di stampante per generare i dati specifici della stampante da inviare poi alla stampante.
4. Dopo che l'incarico di stampa è stato inviato completamente alla stampante, lo spooler della stampante cancella l'incarico dalla queue.

Diversi sistemi di stampa

SuSE Linux Enterprise Server supporta due tipi di sistemi di stampa:

LPRng/lpdfilter – Si tratta di un sistema di stampante tradizionale composto da uno spooler di stampante "LPRng" e di un filtro di stampante "lpdfilter". Nei sistemi di stampa tradizionali la configurazione delle queue viene stabilita dall'amministratore di sistema, ed l'utente può scegliere tra le diverse queue. Al fine di poter scegliere tra diverse configurazioni per una stampante, si devono impostare diverse queue con configurazioni diverse per la stessa stampante. Con le semplici stampanti monocromatiche (per esempio la maggior parte delle stampanti laser) basta una configurazione standard, ma per le moderni stampanti a getto di inchiostro a colori servono configurazioni per stampati monocromatiche, a colori ed eventualmente per stampe policrome e fotostampe ad alta

risoluzione. Attraverso le configurazioni stabilite da una parte viene assicurato che vengono utilizzate solo le configurazioni impostate dal sistemista. Dall'altra però viene preclusa ogni possibilità all'utente di eseguire qualunque impostazione personale. Per l'amministratore di sistema questo significa che deve impostare di conseguenza tante queue, se devono essere reso disponibile l'elevato numero di funzionalità delle stampanti moderni.

CUPS – Nel sistema di stampa CUPS l'utente ha la possibilità di stabilire per ogni stampato impostazioni specifiche della stampante. In questo sistema la configurazione della queue non viene stabilita per intero dall'amministratore di sistema. Le possibilità di impostazioni specifiche della stampante sono deposte per ogni queue in un file sì detto PPD (ingl. *PostScript Printer Description*), e vengono proposte all'utente in una finestra di dialogo della stampante. Le varie possibilità offerte dalla stampante sono deposte nel file PPD; l'amministratore di sistema può comunque modificare il file PPD ed eventualmente limitare le possibilità di configurazione.

Poiché i due sistemi di stampa stanno in conflitto, normalmente non è possibile avere installato entrambi i sistemi di stampa *contemporaneamente*; YaST2 comunque permette di cambiare dall'uno all'altro sistema di stampa – vedi sezione *Configurare la stampante con YaST2* a pagina 61.

Indicazioni generali su problemi di stampante

La documentazione descrive innanzitutto questioni generali e la loro soluzione.

Per tanti problemi specifici trovate una soluzione nella banca dati di supporto (inglese)

Se avete dei problemi con la stampante gli articoli della banca dati di supporto *Installing a Printer* e *Printer Configurtion with SuSE Linux 8.0* rappresentano il punto di partenza che trovate con la parola chiave "Printer" o online sotto:
`http://sdb.suse.de/en/sdb/html/jsmeix_print-einrichten.html`
`http://sdb.suse.de/en/sdb/html/jsmeix_print-einrichten-80.html`
La banca dati di supporto si trova inoltre nel sistema di assistenza di SuSE o online sotto `http://sdb.suse.de/` trovate la versione sempre up-to-date.

I problemi principali rilevati per ogni versione vengono riassunti in un articolo centrale :
Problemi noti e particolarità in SuSE Linux 8.1

http://sdb.suse.de/en/sdb/html/bugs81.html
Problemi noti e particolarità in SuSE Linux 8.0
http://sdb.suse.de/en/sdb/html/bugs80.html
Se non doveste trovare la risposta che cercate né nella documentazione acclusa né nella banca dati di supporto, vi offriamo volentieri assistenza nel quadro del servizio di supporto di SuSE. Per avere ulteriori informazioni andate su
http://www.suse.de/it/services/support/index.html

Premesse

Prerequisiti generali

- La stampante viene supportata da SuSE Linux Enterprise Server? Vedi a riguardo anche le seguenti fonti di informazione:

  Banca dati delle stampanti di SuSE – http://cdb.suse.de o http://hardwaredb.suse.de/ I driver Ghostscript qui descritti corrispondono a quelli che possono essere anche selezionati in YaST2 durante la configurazione della stampante in relazione al modello della stampante

  Linuxprinting.org Banca dati delle stampanti – http://www.linuxprinting.org/ → 'The Database' (http://www.linuxprinting.org/database.html) o http://www.linuxprinting.org/printer_list.cgi

  Ghostscript – http://www.cs.wisc.edu/~ghost/

  SuSE Linux Enterprise Server driver Ghostscript – file:/usr/share/doc/packages/ghostscript/catalog.devices Qui sono elencati i driver Ghostscript che sono effettivamente inclusi nella relativa versione di SuSE Linux Enterprise Server. Questo è importante, poiché a volte su Internet viene indicato un driver Ghostscript che necessita l'attuale versione "Aladdin Ghostscript". In SuSE Linux Enterprise Server è accluso per motivi di licenza "GNU Ghostscript". Di solito vi è anche un driver Ghostscript GNU con il quale la stampante funziona.

- La stampante è fondamentalmente indirizzabile; vedi la sezione *Configurazione manuale di porte di stampanti locali* a pagina 70 o la sezione *Configurazione manuale* a pagina 65.

- Dovreste utilizzare un kernel originale SuSE accluso nel CD-ROM, *non* utilizzate dunque un kernel compilato da voi. In caso di problemi dovreste installare un kernel SuSE originale ed eseguire con questo il reboot.
- Vi raccomandiamo l'installazione del 'Sistema standard' con YaST2, per assicurare che tutti i pacchetti necessari sono disponibili. E' un bene se durante l'installazione del sistema standard non avete disabilitato pacchetti preselezionati. Altrimenti installate almeno il 'sistema standard'. I 'sistemi minimali' non bastono per stampare.

Determinare il driver adatto alla stampante

La stampante PostScript non necessita di speciali driver.

Un driver PostScript genera per stampanti non PostScript i dati specifici di stampa. Per tale ragione è il driver Ghostscript a determinare il risultato delle stampanti non PostScript. La scelta del driver Ghostscript ed eventualmente particolari impostazioni relativi al driver influiscono sul risultato del processo di stampa.

Gli elenchi di cui nella sezione *Prerequisiti generali* nella pagina precedente indicano anche driver Ghostscript per singoli modelli di stampante.

Eventualmente chiedete al produttore della stampante, quale sia il linguaggio della vostra stampante o con quale modello nella banca dati delle stampanti la vostra stampante sia compatibile (vedi sotto). Soprattutto con nuovi modelli di stampanti è facile dire quanto la stampante sia adatta a funzionare sotto Linux. Anche qui le differenze in tema del supporto di Linux dipendono dai vari produttori di stampanti.

Se nemmeno il produttore dovesse essere in grado di fornire delle informazioni sulla vostra stampante riguardo alla compatibilità con Linux, seguite queste indicazioni:

- Accertatevi se la vostra stampante sia compatibile con un modello che gira sotto Linux e utilizzate il driver Ghostscript del modello compatibile.

  Linux compatibile significa che la vostra stampante utilizzando le stesse sequenze di controllo binarie riesce a stampare correttamente come il modello compatibile – cioè le stampante "comprende" lo stesso linguaggio in modo diretto e non ha bisogno di un driver adatto per emularla (per un sistema operativo diverso).

La similitudine nella denominazione delle stampanti, non comporta l'esistenza di una compatibilità. Questo è dovuto al fatto che, a volte, stampanti con una denominazione simile, non comprendono lo stesso linguaggio.

- Quale sia il linguaggio compreso direttamente dalla vostra stampante ve lo potrà dire il produttore. Nel manuale della stampante, tra i dati tecnici, spesso viene indicata il linguaggio della stampante.

  PCL5e o PCL6 – Stampanti che comprendono PCL5e o PCL6 senza intermediazione, dovrebbero funzionare con il driver Ghostscript ljet4 fino a 600x600 dpi. Spesso PCL5e viene indicato solo con PCL5.

  PCL4 o PCL5 – Stampanti che comprendono PCL4 o PCL5, dovrebbero funzionare con i driver Ghostscript: laserjet, ljetplus, ljet2p o ljet3, comunque vi è una restrizione a 300x300 dpi.

  PCL3 Stampanti che comprendono PCL3, dovrebbero funzionare con i driver Ghostscript: deskjet, hpdj, pcl3, cdjmono, cdj500 o cdj550.

  ESC/P2, ESC/P a ESC/P a matrice Stampanti che comprendono direttamente ESC/P2, ESC/P o ESC/P a matrice, dovrebbero funzionare con i driver Ghostscript stcolor o uniprint assieme ad in file parametro adatto *.upp (per esempio stcany.upp).

Stampanti GDI

Dato che i driver delle stampanti per Linux di solito non vengono sviluppati dal produttore dell'hardware, bisogna indirizzare la stampante con un linguaggio generalmente compreso come PostScript, PCL ed ESC/P.

Una stampante normale comprende almeno uno dei linguaggi comunemente usati. Se però il produttore crea una stampante che può essere indirizzata solo con proprie particolari sequenze di controllo, ci troviamo di fronte ad una cosiddetta stampante GDI funzionante solo con la versione del sistema operativo per la quale il produttore acclude il driver. Visto che il modo di indirizzare questo tipo di stampanti non corrisponde a nessuna delle norme conosciute, non è possibile, o solo accompagnato da tante difficoltà, utilizzare sotto Linux questi dispositivi fuori dalla norma.

GDI è una interfaccia di sviluppo concepita dalla Microsoft per la rappresentazione grafica. Il problema non è rappresentato dall'interfaccia di programmazione ma dal fatto che le cosiddette stampanti GDI possono essere indirizzate *solo* attraverso il linguaggio proprietario del relativo modello di

stampante. In fondo l'espressione "stampante indirizzabile *solo* attraverso un linguaggio di stampante proprietario," sarebbe più corretta.

Ve ne sono alcune, tuttavia, il cui hardware non comprende solo il modo GDI, ma -previa configurazione- anche un linguaggio standard. Se accanto ad Linux utilizzate anche un altro sistema operativo, il driver della stampante di quest'ultimo potrà avere innescato eventualmente la modalità GDI nella stampante, in modo da rendere impossibile il funzionamento sotto Linux. Avete due possibilità: riportare la stampante - sotto il sistema operativo installato accanto ad Linux - alla modalità standard, oppure utilizzare - anche sotto l'altro sistema operativo - la stampante solo nella modalità standard, che spesso però comporta una restrizioni delle possibilità di stampa (per esempio una risoluzione minore).

Vi sono inoltre delle particolari stampanti che comprendono solo parte del linguaggio di stampa standard - per esempio solo comandi per l'emissione di dati di grafici a matrice. Questo tipo di stampante a volte può essere utilizzato del tutto normalmente, poiché tanti driver Ghostscript di solito utilizzano solo comandi per l'emissione di dati di grafici a matrice. Eventualmente dei testi in ASCII non potranno essere stampati direttamente dalla stampante ma di default Ghostscript viene sempre frapposto. I problemi con questo tipo di stampanti sorgono solo, se prima devono essere commutate a questo fine con delle sequenze di controllo particolari. Qui non può essere utilizzato alcun driver Ghostscript comune, serve invece un driver adattato che esegue questa commutazione.

Per alcune stampanti GDI esitono driver di casa del produttore. Lo svantaggio è di questi driver Linux *per stampanti GDI* è che non può essere garantito che funzioneranno con le diverse versioni (future) di Linux.

Stampanti comprendenti un linguaggio di stampa standard che è stato pubblicato, non dipendono invece né da un particolare sistema operativo né da particolari versioni di un sistema operativo. Driver Linux fatti in casa dai produttori per questo tipo di stampanti spesso producono i migliori risultati.

Con SuSE Linux Enterprise Server le seguenti stampanti GDI sono supportate direttamente con la configurazione della stampante per mezzo di YaST2; visto che comunque le stampanti GDI causano spesso dei problemi, è possibile che alcuni modelli non funzionano o vi sono delle vistose restrizioni (per esempio solo stampa in bianco e nero a bassa risoluzione). Tenete presente che non possiamo garantire l'affidabilità delle indicazioni che seguono, poiché non sottoponiamo ad alcun test i driver di stampanti GDI (non compriamo stampanti GDI).

- Brother HL 720/730/820/1020/1040, MFC 4650/6550MC/9050 e modelli compatibili.

- HP DeskJet 710/712/720/722/820/1000 e modelli compatibili.
- Lexmark 1000/1020/1100/2030/2050/2070/3200/5000/5700/7000/7200, Z11/42/43/51/52 e modelli compatibili. Driver Linux direttamente di Lexmark si trovano sotto `http://www.lexmark.com/printers/linuxprinters.html`
- Oki Okipage 4w/4w+/6w/8w/8wLite/8z/400w e modelli compatibili.
- Samsung ML-200/210/1000/1010/1020/1200/1210/1220/4500/5080/6040 e modelli compatibili.

Le seguenti stampanti GDI – almeno per quanto ne sappiamo noi – non sono supportate da SuSE Linux Enterprise Server; comunque l'elenco non è completo:

- Brother DCP-1000, MP-21C, WL-660
- Canon BJC 5000/5100/8000/8500, LBP 460/600/660/800, MultiPASS L6000
- Epson AcuLaser C1000, EPL 5500W/5700L/5800L
- HP LaserJet 1000/3100/3150
- Lexmark Z12/22/23/31/32/33/82, Winwriter 100/150c/200
- Minolta PagePro 6L/1100L/18L, Color PagePro L, Magicolor 6100DeskLaser, Magicolor 2 DeskLaser Plus/Duplex
- Nec SuperScript 610plus/660/660plus
- Oki Okijet 2010
- Samsung ML 85G/5050G, QL 85G
- Sharp AJ 2100, AL 1000/800/840/F880/121

Configurare la stampante con YaST2

Queue e configurazione

Sono necessarie più queue per i seguenti motivi:

- Stampanti differenti devono essere indirizzate attraverso queue differenti.
- Il filtro della stampante può essere configurato individualmente per ogni queue; questo significa che vengono utilizzate differenti queue per la stessa stampante per mettere a disposizione differenti configurazioni.

Con stampanti puramente in bianco e nero (per esempio la maggioranza delle stampanti laser) basta una configurazione standard, ma per stampanti a getto di inchiostro policrome servono almeno due tipi di configurazione — e di conseguenza due queue:

- Una configurazione “lp” standard per una stampa veloce e non particolarmente costosa in bianco e nero. Una queue con il nome `lp` non dovrebbe mancare mai, perché si tratta di un nome tradizionale per una queue standard.
- Una configurazione “color” o una queue per stampe a colori.

I principi della configurazione della stampante di YaST2

La configurazione della stampante con YaST2 può essere richiamata non solo attraverso i menu, ma anche come utente `root` direttamente dalla riga di comando con `yast2 printer`. Con `yast2 printer .nodetection` potete evitare il rilevamento automatico della stampante. Vedi a riguardo in particolar modo la sezione *Porte parallele* a pagina 70.

Con la configurazione della stampante di YaST2 vengono configurati *contemporaneamente* entrambi i sistemi di stampa CUPS e LPRng/lpdfilter. Nella banca dati delle stampanti di YaST2 `/usr/lib/YaST2/data/printerdb/suse.prdb` si trovano delle configurazioni per entrambi i sistemi di stampa; comunque non ogni configurazione è disponibile per entrambi i sistemi di stampa. Alcuni tipi di configurazione dunque sono supportate o solo da CUPS o solo da LPRng/lpdfilter, che si evince anche dalla configurazione della stampante di YaST2.

Passare da CUPS e LPRng/lpdfilter è facile grazie ad un ramo del menu estendibile della configurazione della stampante di YaST2. Tipi di configurazione valide per entrambi i tipi di stampa, sono immediatamente disponibili dopo un passaggio all’altro tipo di stampa, però sussistono delle differenze nelle possibilità offerte dal tipo di installazione, in modo che tipi di configurazioni valide per entrambi di sistemi non sono completamente identici per entrambi i sistemi di stampa.

Con la configurazione della stampante di YaST2 potete scegliere tra i seguenti sistema di stampa o passare dall'uno all'altro:

CUPS come server Con una stampante collegata in locale, CUPS deve girare come server. In particolar modo vengono installati per questo sistema di stampa i seguenti pacchetti :

- cups-libs
- cups-client
- cups
- cups-drivers
- cups-drivers-stp

CUPS esclusivamente come client Se nella rete locale vi è un server di rete CUPS, e se si intende stampare solo attraverso le sue queue, è susufficientehe CUPS giri solo come client. Dovete solo indicare il server di rete CUPS. A tal fine bastano i seguenti pacchetti:

- cups-libs
- cups-client

LPRng Se volete usare il sistema di stampa LPRng/lpdfilter o se nella rete locale non vi è alcun server di rete CUPS, ma solo un server di rete LPD (vedi sezione *Lo spooler di stampante LPRng/lpdfilter* a pagina 77) e si intende stampare attraverso la sua queue. In questo caso installate i pacchetti:

- lprng
- lpdfilter

Il pacchetto `cups-client` e il pacchetto `lprng` si escludono a vicenda e non possono essere installati insieme. Il pacchetto `cups-libs` deve essere sempre installato, poiché alcuni programmi (per esempio Samba) hanno un link (per esempio Samba) su librerie CUPS.

Per un sistema di stampa completo servono di solito ulteriori pacchetti che comunque con 'Sistema standard' vengono installati automaticamente – in particolare:

- ghostscript-library
- ghostscript-fonts-std
- ghostscript-x11

- a2ps
- file
- ...

La configurazione della stampante di YaST2 è in grado di funzionare anche senza un sistema di stampa installato, perché salva i file di configurazione sotto `/var/lib/YaST2/printers`. Quando in un secondo momento si installa un sistema di stampa, o se si cambia il sistema di stampa, allora la configurazione della stampante YaST2 genera la configurazione per il sistema di stampa attuale basandosi sui dati salvati sotto `/var/lib/YaST2/printers`.

La configurazione della stampante di YaST2 mostra quale tipo di configurazione potete generare correttamente. Dato che la configurazione viene generata effettivamente solo dopo aver concluso la configurazione della stampante YaST2, ai fini di un controllo si dovrebbe riavviare la configurazione della stampante di YaST2.

La configurazione della stampante di YaST2 distingue nettamente tra queue create con YaST2 (queue di YaST2), e quelle non create con YaST2 (queue nonYaST2). Quest'ultime non possono essere manipolate con YaST2. Dei conflitti si verificano solo nel caso di nomi identici. Questo caso può verificarsi quando per esempio una queue YaST2 "color" è stata generata sotto un sistema di stampa, e poi si passa all'altro sistema di stampa non con YaST2 ma a mano, e lì si genera una queue "color" non con YaST2, ma manualmente, e si inizializza poi la configurazione della stampante di YaST2. In questo caso la queue generata a mano viene sovrascritta dalla omonima queue di YaST2.

Quando si elabora una queue si può scegliere, se per la sua configurazione si vuole usare YaST2 o meno. Trasformando una queue YaST2 in una queue non-YaST2 per esempio si può evitare quanto descritto sopra. Inversamente una queue non-YaST2 può essere convertita in una queue YaST2 ed è possibile sovrascrivere la sua configurazione con la configurazione di YaST2.

Configurazione automatica

A seconda della misura in cui YaST2 rivela automanticamente l'hardware e in qual misura nella banca dati delle stampanti sono presenti informazioni relative alla stampante in questione, YaST2 è in grado di determinare automaticamente i dati necessari ai fini della configurazione o proporne una – in caso contrario l'utente deve fornire i dati richiesti immettendoli nei dialoghi.

YaST2 consente la configurazione automatica della stampante, se vengono soddisfatte queste condizioni:

- Con la rivelazione automatica dell'hardware, la porta parallela o la porta USB può essere impostata correttamente in modo automatico e la stampante ad essa collegata può essere rilevata automaticamente.
- Nella banca dati della stampante vi è l'ID del modello della stampante, che YaST2 ha ottenuto durante il rilevamento automatico dell'hardware. Visto che questo ID può discostarsi dalla denominazione del modello, può darsi che il modello deve essere scelto manualmente.
- Per il modello in questione si deve inserire almeno un tipo di configurazione nella banca dati di supporto che funziona senza difficoltà alcuna ed è valida per entrambi i sistemi di stampa, ovvero CUPS e LPRng/lpdfilter.

Per ogni tipo di configurazione bisognerebbe eseguire un test di stampa di YaST2 per verificare il corretto funzionamento, anche perché in molti casi il tipo di configurazione va inserito nella banca dati delle stampanti senza supporto esplicito da parte del produttore, e così non è possibile garantire il funzionamento per ogni immissione.

Inoltre il test di stampa con YaST2 fornisce importanti informazioni sulla relativa configurazione.

Configurazione manuale

Nel caso in cui una delle condizioni per la configurazione automatica non viene soddisfatta o se si desidera un tipo di configurazione particolare - per così dire su misura - le impostazioni vanno eseguite manualmente.

I seguenti valori devono essere configurati:

Connessione dell'hardware (porta)

- Se YaST2 rivela automaticamente il modello di stampa, si può presumere che la connessione della stampa funzione a livello dell'hardware, e che dunque non serve configurare delle impostazioni.
- Se però YaST2 non rivela automaticamente il modello della stampante, ciò indica che la connessione della stampante funziona a livello dell'hardware solo previa configurazione manuale.

  `/dev/lp0` è la prima porta parallela
  `/dev/usb/lp0` è la porta per una stampante USB

  Configurando manualmente si deve scegliere la porta. In questi casi va assolutamente eseguito il relativo test in YaST2 per

controllare se la stampante è indirizzabile attraverso la porta scelta.

Il modo più sicuro in questi casi è connettere la stampante direttamente alla prima porta parallela e settare nel BIOS le seguenti impostazioni per la porta parallela:

- Indirizzo IO 378 (esadecimale)
- L'interrupt non è rilevante
- Modo `Normal`, `SPP` o `Output-Only`
- Senza DMA

Se nonostante queste impostazioni nel BIOS la stampante non risulta essere indirizzabile attraverso la prima porta parallela, allora nelle impostazioni dettagliate per la porta parallela deve essere inserito in modo esplicito l'indirizzo IO `0x378` - in corrispondenza alle impostazioni nel BIOS. Se esistono due porte parallele impostate sugli indirizzi IO 378 e 278 (esadecimale), allora devono essere inseriti nel seguente modo: `0x378,0x278`. Vedi a riguardo in particolar modo la sezione *Porte parallele* a pagina 70.

Nome della queue Dato che spesso va indicato il nome della queue per stampare, usate solo nomi brevi composti da minuscole ed eventualmente numeri.

Con il sistema di stampa LPRng/lpdfilter sussistono le particolari possibilità di configurazione riportate di seguito:

- Per casi particolari potete settare una cosiddetta queue `raw`. Nella queue `raw` il filtro della stampante non converte i dati da stampare, essi vengono inviati direttamente nello stato grezzo alla stampante. Per questo motivo, se utilizzate una queue `raw` i dati da stampare devono essere già disponibili nel linguaggio della stampante.
- Potete impostare la queue con o senza formfeed, a seconda se lo spooler dopo ogni processo di stampa innesca in modo esplicito un avanzamento di modulo, in modo da emettere anche l'ultimo foglio dell'incarico. Normalmente se ne occupa il driver Ghostscript, allora non serve alcun avanzamento.

Driver Ghostscript e linguaggio della stampante Il driver Ghostscript e linguaggio della stampante vengono determinati dal modello della stampante e vengono stabiliti attraverso la scelta di una configurazione predefinita, che si lascia all'occorrenza modificare in una maschera a parte, adatta al modello della stampante.

Dato che il driver Ghostscript genera dati da stampare per stampanti non PostScript, la configurazione del driver Ghostscript è il punto cruciale per determinare il tipo di stampato. In primo luogo è la scelta del driver Ghostscript a determinare le caratteristiche dello stampato e poi le impostazioni driver adatte. Qui vengono impostate le caratteristiche e le differenze dello stampato tra i diversi tipi di configurazione che saranno applicate alla stampante.

Se YaST2 ha rilevato automaticamente il modello della stampante o il modello è incluso nella banca dati delle stampanti, vi è una preselezione di driver Ghostscript adatti. In questo caso YaST2 mette a disposizione diversi tipi di configurazionen predefiniti – per esempio

- Stampa in bianco e nero 300 dpi
- Solo LPRng: stampato con graduazione dei grigi 300 dpi
- Stampa a colori 300 dpi
- Solo CUPS: stampa a colori 600 dpi
- Fotostampa 600 dpi

In questi casi YaST2 mostra anche se un tipo di configurazione venga supportato solo da uno dei due sistemi di stampa, ovvero CUPS o LPRng/lpdfilter.

La configurazione predefinita contiene un driver Ghostscript proprio ed eventualmente impostazioni driver adatti al tipo di stampato in questione.

Nel caso vi siano impostazioni del driver, le potete modificare in una maschera separata.

Le voci di menu indentate indicano il nesso tra valore selezionato e le possibilità offerte dalla sottoselezione.

Non tutte le combinazioni di impostazioni driver tra cui potete scegliere, funzionano in modo indiscriminato con ogni modello di stampante – soprattutto in combinazione con una elevata risoluzione.

Consigliamo vivamente di eseguire un test della stampante con YaST2. Se questo tentativo non dovesse produrre il risultato atteso (per esempio tanti fogli quasi vuoti), potete fermare il processo togliendo tutti fogli e dopo interrompendo il test. A volte in seguito non è più possibile stampare. Dunque è meglio interrompere il test e lasciare che il foglio in fase di stampa venga emesso.

Se il modello della stampante non è contenuto nella banca dati, avete comunque una selezione di driver Ghostscript generici per linguaggi di stampante standard.

Se volete usare un driver Ghostscript non presente nella preselezione, vi è un "produttore" sotto il quale il driver Ghostscript può essere selezionato in modo individuale.

Per il sistema di stampa CUPS vi sono le seguenti possibilità:

- Per il sistema di stampa CUPS vengono di solito utilizzate file PPD sotto `/usr/lib/YaST2/data/printerdb/`, perché devono adattarsi perfettamente alle registrazioni nella banca dati delle stampanti di YaST2. I file PPD di YaST2 si basano sui corrispondenti file PPD dal pacchetto `cups-drivers` e dal pacchetto `cups-drivers-stp`. Se selezionate il modello della stampante manualmente, si può selezionare al posto del modello della stampante (cioè al posto di un file PPD YaST2) un qualsiasi file PPD, dunque per esempio un file PPD dai pacchetti cups-drivers e cups-drivers-stp sotto `/usr/share/cups/model/`. Dato che però per file PPD non vi è una registrazione nella banca dati delle stampanti di YaST2, le preimpostazioni del file PPD non possono essere modificati con YaST2. Comunque vi è un modo di modificarle che viene descritto nella sezione *Impostazione della queue* a pagina 105.

Altre impostazioni speciali Potete intervenire su queste impostazioni tramite un procedimento particolare e in caso di dubbio conviene non modificare le impostazioni di default.

Per il sistema di stampa CUPS vi sono le seguenti impostazioni:

- Limitazione dell'accesso per determinati utenti.
- Stato della queue: se concludere il processo di stampa o meno; se la queue debba accettare incarichi di stampa o meno.
- Pagine con banner o frontespizi: se e quali pagine con banner debbano essere stampate prima della stampa vera e propria e se e quando le pagine banner devono essere stampate dopo il processo vero e proprio.

Il sistema di stampa LPRng/lpdfilter offre le seguenti particolari impostazioni valide per ogni hardware:

- Si può stabilire il layout della pagina per la stampa di testi ASCII, non solo per grafiche e documenti generati con particolari applicativi.
- Per casi particolari la queue può essere impostata quale queue sì detta `ascii` che forza il filtro della stampante a emettere testo ASCII. Questo è necessario per forzare nel caso di file di testo

ASCII non rilevate dal filtro come tali l'emissione di testo ASCII (p.e. per stampare sorgenti di PostScript).

- La codificazione nazionale riguarda la raffigurazione di caratteri speciali della stampa di testi ASCII e testo semplice nelle pagine HTML di Netscape.

Configurazione per applicativi

Applicativi utilizzano queue esistenti a mo della riga comando per quanto riguarda la stampa. Per tale motivo negli applicativi non viene configurata la stampante ma la queue esistente.

Stampare sulla riga di comando

Con la riga di comando si stampa attraverso il comando `lpr -Plp Nomefile`, dove `NOMEFILE` deve essere sostituito con il nome del file da stampare. In questo caso viene usata la queue standard `lp`. Attravero l'opzione `-P` si può determinare esplicitamente la queue. Con `lpr -Pcolor NOMEFILE` viene usata per esempio la queue `color`.

Con il sistema di stampa LPRng/lpdfilter

Gli applicativi utilizzano in questo caso il comando `lpr` per stampare. Inoltre scegliete un nome nell'applicativo di una queue esistente (per esempio `lp` o `color`) oppure immettete nella maschera per stampare dell'applicativo il comando per stampare adatto (per esempio `lpr -Plp` o `lpr -Pcolor`).

Con il sistema di stampa CUPS

Il pacchetto `cups-client` contiene tool di righe di comando per stampare con CUPS, come per esempio il comando `lpr`, in modo che quanto detto sopra funzioni anche per CUPS.

Inoltre vi sono programmi di stampante grafici come xpp o il programma KDE `kprinter` che consentono non solo di scegliere la queue, ma anche di impostare opzioni standard CUPS ed opzioni specifici per la stampa dal file PPD tramite i menu di selezione grafici.

Configurazione manuale di porte di stampanti locali

Porte parallele

Di solito una stampante si collega ad un sistema Linux attraverso una porta parallela. Una stampante collegata alla porta parallela viene indirizzata attraverso il sottosistema `parport` del kernel.

La configurazione di base di una porta parallela con YaST2 viene descritta nella sezione *Configurazione manuale* a pagina 65, per questo riportiamo qui solo informazioni basilari:

Attraverso il caricamento di moduli di kernel di una specifica architettura si devono far conoscere al sottosistema `parport` le porte parallele. Così da fare funzionare *contemporaneamente* diversi dispositivi collegati a catena (per esempio un lettore ZIP da porta parallela ed una stampante) allacciati ad *una* porta parallela. Il conteggio dei file di dispositivo per stampanti da porta parallela inizia con `/dev/lp0`. Per poter stampare tramite la prima porta parallela, con il kernel standard di SuSE si devono caricare i moduli `parport`, `parport_pc` e `lp`. Questo viene fatto di solito automaticamente da kmod (ingl. *Kernel Module Loader*), non appena si accede per la prima volta su un file di dispositivo (per esempio `/dev/lp0`).

Se il modulo del kernel `parport_pc` viene caricato senza parametri speciali, cercherà di rilevare e configurare automaticamente la porta parallela. In casi rari non funziona, e si può verificare un immediato blocco del sistema. A questo punto bisogna configurare i parametri corretti per il modulo `parport_pc` a mano. Per tale motivo, come descritto nella sezione *Configurare la stampante con YaST2* a pagina 61, con YaST2 si lascia evitare il rilevamento automatico della stampante.

Configurazione manuale della porta parallela

La porta parallela `/dev/lp0` viene configurata attraverso la registrazione in `/etc/modules.conf` (file 2).

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=none
```

file 2: */etc/modules.conf: prima porta parallela*

Accanto ad `io` si vede l'indirizzo IO della porta parallela.

Accanto ad `irq` c'è `none` quale preimpostazione per il funzionamento nella modalità "Polling" o l'interrupt delle porte parallele. Il polling è meno problematico dell'Interrupt, dal momento che si possono evitare conflitti di interrupt. Comunque vi sono delle motherboard e/o stampanti che funzionano correttamente solo nella modalità Interrupt; inoltre questa modalità fa sì che la stampante riceva abbastanza dati anche sotto se il sistema è molto carico.

Affinché queste impostazioni funzionino, nel BIOS o attraverso il firmware del PC dovrete impostare per la porta parallela i seguenti valori (se disponibili):

- Indirizzo IO `378` (esadecimale)
- Interrupt `7` (irrelevante nella modalità Polling)
- Modus `Normal`, `SPP` o `Output-Only` (altre modalità non sempre funzionano)
- `DMA` è disabilitato (lo dovrebbe essere nella modalità `Normal`)

Se l'Interrupt `7` è ancora libero, allora con

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

file 3: */etc/modules.conf: modalità Interrupt per la prima porta parallela*

la modalità Interrupt può essere attivata. Prima di attivare la modalità Interrupt, con

```
terra:~ #  cat /proc/interrupts
```

bisogna determinare quali Interrupt sono già utilizzati; qui vengono mostrati solo gli Interrupt che vengono utilizzati al momento, il che può variare dall'hardware attivamente in uso. L'Interrupt per la porta parallela non può essere già utilizzato. Se non siete certi, utilizzate la modalità Polling.

Configurazione di altre porte parallele

Una seconda interfaccia parallela `/dev/lp1` indirizzabile all'indirizzo IO standard 278 (esadecimale) (impostabile, ad esempio, con un jumper su una scheda interfaccia ISA), può essere configurata anche in `/etc/modules.conf` (file 4).

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378,0x278 irq=none,none
```

file 4: */etc/modules.conf: due porte parallele*

Schede ad innesto speciali: ISA-PnP e PCI

Se non è ancora conosciuto, dovrete determinare l'indirizzo IO di un'interfaccia parallela supplementare.

Schede ISA PnP Se potete impostare su queste schede un valore fisso per l'indirizzo IO e, eventualmente, per l'interrupt ed il modo (per esempio, con un jumper), fatelo.

Altrimenti, i valori per l'indirizzo IO, interrupt e modo vengono registrati sulla scheda ISA PnP, all'avvio di Linux. Quali valori debbano venire registrati, lo si può vedere nelle comunicazioni del boot di Linux (nel file `/var/log/boot.msg`) oppure con l'aiuto del comando `pnpdump` (pacchetto `isapnp`)

Schede PCI Quali indirizzi IO e quale interrupt siano adatti per una scheda PCI, si può appurare con il seguente comando (vd. l'output *Schede ad innesto speciali: ISA-PnP e PCI* in questa pagina):

```
terra:~ #  /sbin/lspci -v


00:0a.0 Parallel controller: ...
        ... IRQ 10
        I/O ports at b400
        I/O ports at b000
        I/O ports at a800
        I/O ports at a400
```

output 1: *Parte di* `lspci -v` *per una scheda interfaccia PCI*

Sempre due indirizzi IO con un intervallo di 400 (esadecimale) appartengono entrambi ad una porta parallela – nel nostro esempio la porta ha b000 e b400 e l'altra a400 e a800. Eventualmente va testato con quale dei due indirizzi funzioni effettivamente e la registrazione di configurazione in `/etc/modules.conf` può essere simile al file 5.

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378,0xb400,0xa800 irq=none,none,none
```

file 5: */etc/modules.conf: scheda PCI con due porte parallele*

Attivazione e test di un'interfaccia parallela

Dopo il riavvio, sarà pronta l'interfaccia parallela.

Al posto di un reboot, è sufficiente, come utente `root`, attualizzare la lista delle dipendenze dei moduli del kernel e scaricare i moduli del kernel necessari all'interfaccia parallela....

```
terra:~ #  depmod -a 2>/dev/null
terra:~ #  rmmod lp
terra:~ #  rmmod parport_pc
terra:~ #  rmmod parport
```

...e ricaricare:

```
terra:~ #  modprobe parport
terra:~ #  modprobe parport_pc
terra:~ #  modprobe lp
```

Se la stampante può riprodurre testi ASCII, entrare nel sistema come `root` e dare il comando

```
terra:~ #  echo -en "\rHello\r\f" >/dev/lp0
```

per stampare una pagina con la parola `Hello`.

La parola `Hello` è, nell'esempio, affiancata dal simbolo ASCII \r, che codifica il capoverso e seguita dal simbolo ASCII \f, che codifica un formfeed.

Per una seconda interfaccia parallela, selezionate `/dev/lp1`; per una terza, selezionate `/dev/lp2`.

Collegamento USB

Nel BIOS del computer, deve essere attivato un interrupt per l'USB. Con un Award-BIOS, per esempio, si deve impostare 'USB IRQ' nel menù 'PNP AND PCI SETUP' su `Enabled`. A seconda della versione BIOS vengono utilizzate anche altri termini.

Immettendo, come utente `root` :

```
terra:~ #  echo -en "\rHello\r\f" >/dev/usb/lp0
```

provate se la stampante USB è indirizzabile.

Se una sola stampante USB è collegata e la stampante è in grado di stampare caratteri ASCII, dovrebbe venire stampata una pagina con la parola `Hello`.

Alcune stampanti necessitano una sequenza di controllo speciale, prima di accettare dati tramite USB. Il seguente comando invia la seguenza di controllo adatta a stampanti USB Epson Stylus Color (immettete il comando su una sola riga senza spazi o ritorni a capo):

```
echo -en "\x0\x0\x0\x1b\x01\x40\x45\x4a\x4c
\x20\x31\x32\x38\x34\x2e\x34\x0a\x40\x45\x4a\x4c\x20
\x20\x20\x20\x20\x0a" >/dev/usb/lp0
```

Ulteriori informazioni le trovate anche nella banca dati di supporto con la parola chiave “Epson” e “usb”.

Nell’output del seguente comando dovrebbe esservi il produttore e il nome della stampante:

```
terra:~ #  cat /proc/bus/usb/devices
```

Se non vengono indicati né il produttore né il prodotto, di solito sono queste le cause:

- Il sistema USB non ha (ancora) rilevato il dispositivo – forse perché la stampante USB è spenta. La stampante USB così non è indirizzabile.
- Il sistema USB ha sì rilevato il dispositivo, ma non conosce né il produttore né il nome della stampante e quindi non mostra nulla. La stampante USB è comunque indirizzabile.

A volte succede che la stampante USB non risponda più (per esempio, se si stacca lo spinotto USB). Di solito, dovrebbero bastare questi comandi, per riavviare il sistema USB:

```
terra:~ #  rchotplug stop
terra:~ #  rchotplug start
```

Se non basta, terminate tutti i processi che accedono a `/dev/usb/lp0` e scaricate e ricaricate i moduli del kernel che riguardano le stampanti USB. Con `lsmod` controllate prima quali moduli USB siano caricati (se `usb-uhci` o `usb-ohci` o `uhci`) o se ci siano ancora altre dipendenze di moduli, ad esempio la segnalazione.

```
usbcore  ...  [printer usb-uhci]
```

indica che il modulo `usbcore` è ancora necessario ai moduli `printer` ed `usb-uhci`. Perciò, in questo caso, prima del modulo `usbcore`, devono venire scaricati i moduli `printer` ed `usb-uhci`. Immettete come `root` i seguenti comandi (al posto di `usb-uhci` a secondo del sistema anche `uhci` o `usb-ohci`):

```
terra:~ #  fuser -k /dev/usb/lp0
terra:~ #  rchotplug stop
terra:~ #  rmmod printer
terra:~ #  rmmod usb-uhci
terra:~ #  umount usbdevfs
terra:~ #  rmmod usbcore
terra:~ #  modprobe usbcore
terra:~ #  mount usbdevfs
terra:~ #  modprobe usb-uhci
terra:~ #  modprobe printer
terra:~ #  rchotplug start
```

Se sono connessi diverse stampanti USB, bisogna considerare quanto segue: il sottosistema USB rivela automaticamente stampanti USB connesse. La prima stampante USB rilevata, è indirizzabile tramite il dispositivo `/dev/usb/lp0`. La seconda stampante USB rilevata, è indirizzabile tramite il dispositivo `/dev/usb/lp1`. Alcuni modelli di stampante vengono rilevati automaticamente anche quando sono spente; ciò è dovuto al fatto che alcune stampanti anche spente, possono essere interrogate tramite il collegamento USB. Per evitare di perdere la visione di insieme per quanto rigurda i dispositivi USB, prima di avviare Linux tutte le stampanti USB dovrebbero essere accese e possibilmente rimanere tali durante il funzionamento.

Interfaccia della stampante IrDA

Una interfaccia parallela viene emulata tramite il collegamento ad infrarossi. Il driver nel kernel Linux mette a disposizione un'interfaccia parallela simulata sotto il dispositivo `/dev/irlpt0`. Una stampante dunque viene indirizzata allo stesso modo come una stampante alla porta parallela con la sola differenza che viene utilizzata `/dev/irlpt0` al posto di `/dev/lp0`.

Provate se la stampante IrDA è indirizzabile immettendo come utente root:

```
terra:~ #  echo -en "\rHello\r\f" >/dev/irlpt0
```

Premesso che la stampa riesca a stampare caratteri ASCII, allora dovrebbe venir prodotta una pagina con la parola `Hello`.

Ad ogni caso la stampante dovrebbe apparire nell'output del seguente comando:

```
terra:~ #  irdadump
```

Altrimenti la stampante non è indirizzabile.

Se non viene indicato proprio niente, allora probabilmente il servizio di sistema IrDA non è sarà stato inizializzato, perché non viene inizializzato automaticamente all'avvio. Con

```
terra:~ #  rcirda start
terra:~ #  rcirda stop
```

potete inizializzare o terminare il servizio di sistema IrDA.

Interfaccia seriale

Il funzionamento della stampante collegata ad un'interfaccia seriale per quanto riguarda lo spooler viene descritto nel *LPRng-Howto* sotto `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html` e lì in particolar modo in `file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#SECSERIAL` e nella pagina di manuale di `printcap` (`man printcap`). Nella banca dati di supporto trovate ulteriori informazioni avviando una ricerca immettendo il termine "seriale".

Configurazione manuale di LPRng/lpdfilter

Di solito il sistema di stampa viene configurato con YaST2, come descritto nella sezione *Configurare la stampante con YaST2* a pagina 61.

Inoltre per il sistema di stampa LPRng/lpdfilter esiste il programma lprsetup basato sulla riga di comando. Quando una stampante viene configurata con YaST2, esso raccoglie le informazioni necessarie e richiama lprsetup con le opzioni necessarie per configurare il sistema di stampa LPRng/lpdfilter.

Il programma lprsetup è stato ideato come tool per “esperti”. A differenza di YaST2, lprsetup non aiuta l’utente a trovare i valori giusti per le singole opzioni.

Con `lprsetup -help` vengono elencate e descritte le opzioni possibili, e ulteriori informazioni sono reperibili nella pagina di manuale di `lprsetup` (`man lprsetup`) o pagina di manuale di `lpdfilter` (`man lpdfilter`).

Per avere informazioni su driver Ghostscript e parametri specifici del driver vedi sezione *Determinare il driver adatto alla stampante* a pagina 58 e *Su Ghostscript* a pagina 107.

Lo spooler di stampante LPRng/lpdfilter

Come spooler di stampante del sistema di stampa LPRng/lpdfilter viene utilizzato il pacchetto `lprng`.

Lo spooler della stampante lpd (ingl. *Line Printer Daemon*) normalmente viene attivato automaticamente all’avvio del sistema, richiamando lo script `/etc/init.d/lpd`. Manualmente lo spooler della stampante - che gira come Daemon in sottofondo - può essere inizializzato e terminato:

```
terra:~ #  rclpd start
terra:~ #  rclpd stop
```

I file di configurazione per il LPRng sono:

/etc/printcap Configurazione delle singole queue

/etc/lpd.conf Configurazione complessiva dello spooler

/etc/lpd.perms Configurazione dei diritti di accesso

Con `rclpd start` viene richiamato in linea con `/etc/init.d/lpd` anche `checkpc -f` che genera le directory spool `/var/spool/lpd/*` attenedosi alle registrazioni in `/etc/printcap` e imposta i diritti d’accesso.

Lo spooler della stampante stabilisce all’avvio, basandosi sulle registrazioni in `/etc/printcap` quali queue vengono definite. Il suo compito è quello di organizzare l’esecuzione li incarichi temporaneamente memorizzati:

- Amministra le queue locali, invia i file dati di un incarico attraverso il filtro della stampante e in seguito o direttamente alla stampante o li inoltra ad una queue diversa.

- Tiene in considerazione la sequenza degli incarichi nella queue.
- Controllo lo stato delle queue e della stampante, e fornisce le informazioni richiesti.
- Ascolta alla porta 515 se sono in arrivo incarichi per la stampante da computer remoti per le queue locali da accettare o eventualmente rifiutare.
- Inoltra gli incarichi da stampare a queue su computer remoti a e quello spooler di quella stampante (dunque la porta 515 del computer remoto).

Per i dettagli sullo spooler LPRng leggete *LPRng-Howto* sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html`
La pagina di manuale di `printcap` (`man printcap`) e la pagina di manuale di `lpd` (`man lpd`).

Tool di riga di comando per il LPRng

I tool di riga di comando vengono descritti dettagliatamente nel *LPRng-Howto* sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPRNGCLIENTS`
così qui riportiamo solo un breve riassunto:

Per queue locali

Generare incarichi di stampa

Il comando `lpr` viene descritto nel *LPRng-Howto* sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPR`
in questa sede riportiamo solo le nozioni fondamentali:

Normalmente si stampa con

```
tux@terra:~ >  lpr -P⟨queue⟩ ⟨file⟩
```

Ommettendo l'opzione `-P`⟨*queue*⟩, il default è il contenuto della variabile di ambiente `PRINTER`. Questo vale anche per i comandi `lpq` e `lprm` – vedi la pagina di manuale di `lpr` (`man lpr`), pagina di manuale di `lpq` (`man lpq`) e la pagina di manuale di `lprm` (`man lprm`). La variabile di ambiente `PRINTER` viene impostata automanticamente al login, e può essere visualizzata con il comando `echo $PRINTER` e con

```
tux@terra:~ >  export PRINTER=⟨queue⟩
```

venir impostata su un'(altra) queue.

Mostrare lo stato

```
tux@terra:~ >  lpq -P⟨queue⟩
```

mostra gli incarichi per la stampa nella queue indicata. Come nel caso dello spooler LPRng immettete `all` come queue, e vengono elencati tutti gli incarichi in tutte le queue.

Con `lpq -s -P`⟨*queue*⟩ vengono mostrate informazioni minimali; con `lpq -l -P`⟨*queue*⟩ le informazioni fornite sono più corpose.

Con `lpq -L -P`⟨*queue*⟩ viene emesso un rapporto sullo stato dettagliato che serve alla individualizzazione di fonti di errore.

Per ulterioi informazioni vedi sotto la sezione *Mostra lo stato di queue remote*, la pagina di manuale di `lpq` (`man lpq`) ed infine
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPQ`
nel *LPRng-Howto*.

Cancellare incarichi di stampa

```
tux@terra:~ >  lprm -P⟨queue⟩ ⟨numero dell'incarico⟩
```

cancella l'incarico specificato dalla queue indicata se l'incarico appartiene all'utente che ha immesso il comando `lprm`. L'incarico appartiene all'utente sul computer che ha inviato l'incarico. Questo utente si lascia identificare con il comando `lpq` che mostra anche il numero dell'incarico.

Con il comando

```
terra:~ #  lprm -Pall all
```

vengono cancellati tutti gli incarichi di tutte le queue per i quali ha il permesso l'utente che ha immesso il comando `lprm`. L'utente `root` può cancellare ogni incarico (anche in tutte le queue).

Ulteriori informazioni nella pagina di manuale di `lprm` (`man lprm`) e sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPRM`
nel *LPRng-Howto*.

Controllo delle queue

`tux@terra:~ >` **`lpc option`** ⟨***queue***⟩

mostra lo stato delle queue indicate e consente di modificarle.

Le opzioni principali sono:

`help` dà un sommario delle opzioni.

`status` ⟨*queue*⟩ emette il rapporto sullo stato.

`disable` ⟨*queue*⟩ rifiuta nuovi incarichi.

`enable` ⟨*queue*⟩ abilita la queue ad accettare nuovi incarichi.

`stop` ⟨*queue*⟩ ferma il processo di stampa degli incarichi della queue; l'incarico che si trova in fase di stampa viene ancora terminato.

`start` ⟨*queue*⟩ riprende con il stampare degli incarichi della queue.

`down` ⟨*queue*⟩ ha l'effetto di `disable` più `stop` .

`up` ⟨*queue*⟩ ha l'effetto di `enable` più `start` .

`abort` ⟨*queue*⟩ è identico a `down`, con la sola differenza che l'incarico che si trova in fase di stampa viene interrotto. Questi incarichi rimangono validi e possono essere terminati dopo un riavvio della queue (`up`).

Per modificare la queue dovete agire da `root`.

Potete immettere i comandi nella riga di comando (per esempio `lpc status all`), o richiamate `lpc` senza parametri: viene inizializzato il modo dialogo con il prompt lpc> che aspetta l'immissione delle opzioni di cui sopra. Con `quit` o `exit` terminate il dialogo.

Se per esempio `lpc status all` emette

```
Printer         Printing Spooling Jobs Server Subserver
lp@earth         enabled  enabled    2    123       456
color@earth     disabled disabled    0   none      none
laser@earth     disabled  enabled    8   none      none
```

vuol dire che la queue `lp` è attivata e contiene due incarichi, di cui uno si trova in fase di stampa. La queue `color` è disattivata. Nella queue `laser`, per esempio per motivi di manutenzione della stampante, è disattivata solo

l'emissione di stampe, ma è possibile stampare degli incarichi raccolti nella queue (nel nostro esempio: 8).

Ulteriori informazioni si trovano nella pagina di manuale di `lpc` (`man lpc`) e sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#LPRM`
nella *LPRng-Howto*.

Per queue remote

Qui dovete sostituire `print-server` con il nome o l'indirizzo IP del server della stampante, e ⟨*queue*⟩ deve essere una queue sul server della stampante.

Generare incarichi di stampa

Con lo spooler LPRng si può accedere a queue remote con il comando `lpr`:

```
tux@terra:~ >  lpr -P⟨queue⟩@server della stampante ⟨file⟩
```

La premessa è che il server della stampante sia stato configurato in modo che sia possibile utilizzare le sue queue, cosa possibile come standard con LPRng.

Mostrare lo stato

Con il comando

```
tux@terra:~ >  lpq -P⟨queue⟩@print-server
tux@terra:~ >  lpq -s -P⟨queue⟩@server della stampante
tux@terra:~ >  lpq -l -P⟨queue⟩@server della stampante
tux@terra:~ >  lpq -L -P⟨queue⟩@server della stampante
```

e

```
tux@terra:~ >  lpc status ⟨queue⟩@server della stampante
tux@terra:~ >  lpc status all@server della stampante
```

può interrogare le queue remote.

Soprattutto con `lpq -s -Pall@server della stampante` o `lpc status all@print-server` possono venire rilevati i nomi di tutte le queue sul server della stampante, se anche sul server della stampante viene utilizzato LPRng.

Se non è possibile stampare su queue remote, una interrogazione sullo stato può dare utili indicazioni.

Con `lpq -L -P⟨queue⟩@server della stampante` può essere visualizzato un rapporto sullo stato ai fini della diagnosi a remoto, se anche sul server della stampante viene utilizzato LPRng.

Cancellare incarichi di stampa

Con i comandi

```
tux@terra:~ >  lprm -P⟨queue⟩@server della stampante ⟨numero
     dell'incarico⟩
tux@terra:~ >  lprm -P⟨queue⟩@server della stampante all
tux@terra:~ >  lprm -Pall@server della stampante all
```

potrete cancellare tutti gli incarichi su queue remote che avete generato voi. In particolare, `root` non ha alcun tipo di privilegi nei confronti di queue remote.

`all` funziona solo se anche sul server della stampante viene utilizzato LPRng.

Eliminare disfunzioni con il comando descritto sopra in LPRng

Gli incarichi di stampa rimangono nella queue anche quando viene eseguito lo shutdown del computer durante il processo di stampa e riavviate Linux – un incarico di stampa contenente degli errori va rimosso dalla queue con i comandi riportati sopra.

Se per esempio si verifica un guasto per quanto riguarda la comunicazione tra computer e stampante, la stampante non è in grado di elaborare i dati che le sono stati inviati e come risultato vengono riempiti con caratteri senza significato innumerevoli fogli.

1. Con stampanti a getto di inchiostro togliete innanzitutto i fogli o nel caso di stampanti laser aprite il cassetto dei fogli per fermare il processo di stampa.
2. Visto che l'incarico viene rimosso dalla queue solo dopo essere stato inviato completamente alla stampante, lo si ritroverà nella maggior parte dei casi ancora nella queue. Controllate con `lpq` o `lpc status` quale incarico da quale queue si trova attualmente nel processo di stampa, e cancellate l'incarico con `lprm`.
3. Può verificarsi che vengono trasmessi dei dati alla stampante anche se l'incarico è stato cancellato dalla queue. Tutti processi che accedono ancora alla stampante vengono terminati con il comando `fuser -k /dev/lp0` per stampanti alla porta parallela e con `fuser -k /dev/usb/lp0` per una stampante USB.
4. Eseguite un reset della stampante staccando per alcuni minuti la spina, ed in seguito rimettete i fogli e accendete la stampante.

Il filtro della stampante del sistema di stampa LPRng/lpdfilter

Come filtro della stampante viene utilizzato lpdfilter (pacchetto `lpdfilter`).

Segue una descrizione dettagliate della elaborazione di un incarico di stampa. Per una analisi dettagliata dei filtri, leggete i script del filtro (in particolare `/usr/lib/lpdfilter/bin/if`) ed eventualmente procedete come descritto nella sezione *Ricerca degli errori nel lpdfilter* a pagina 91.

1. Il filtro (`/usr/lib/lpdfilter/bin/if`) determina le opzioni che desume dallo spooler, leggendole dal cosiddetto “control file” degli incarichi, nonché, a seconda delle queue, dai file `/etc/printcap` e `/etc/lpdfilter/`⟨*queue*⟩`/conf` (⟨*queue*⟩ va sostituito con il nome della queue).

2. Viene determinato il tipo di dati da stampare. Con `/usr/lib/lpdfilter/bin/guess`, viene applicato il comando `file` ai dati da stampare. Con il suo output e sulla base dei valori nel file `/etc/lpdfilter/types`, viene fissato il tipo di dati da stampare.

   - Se si tratta di una queue `ascii`, il filtro viene costretto a trattare i dati da stampare come caratteri ASCII.
   - Se non si tratta di una queue `ascii`, il filtro cerca di determinare automaticamente il tipo di dati da stampare.

3. A seconda del tipo di dati e di queue, avviene ora la conversione in dati specifici della stampa:

   - Se si tratta di una queue `raw`, i dati da stampare vengono inviati direttamente alla stampante (o ad un’altra queue); se le impostazioni in `/etc/lpdfilter/`⟨*queue*⟩`/conf` lo prevedono, essi possono anche venire ricodificati con recode Per una `raw` queue assoluta (ovvero senza lpdfilter), cancellate per la queue in questione, la riga `:if=/usr/lib/lpdfilter/bin/if:\` su `/etc/printcap`.
   - Se non si tratta di una `raw` queue:

     (a) Se i dati da stampare non sono PostScript, lo diventeranno richiamando `/usr/lib/lpdfilter/filter/tipo2ps` (laddove `typ` venga sostituito dal tipo di dati da stampare). I testi ASCII, in particolare, vengono tradotti in PostScript secondo `/usr/lib/lpdfilter/filter/ascii2ps`, con il

programma a2ps e sulla base della codificazione nazionale configurata per la queue. In questo modo, tutti i caratteri speciali saranno stampabili correttamente anche in un semplice formato di testo; vd. anche pagina di manuale di `a2ps` (`man a2ps`).

(b) I dati PostScript possono anche essere riformattati, a condizione che, sotto `/etc/lpdfilter/`⟨*queue*⟩`/pre` vi sia uno script adatto (laddove `queue` sia da sostituire con il nome della queue).

(c) I dati PostScript possono anche essere tradotti in un altro linguaggio.

- ▷ Se la stampante è PostScript, i dati in PostScript vengono inviati direttamente ad essa (o ad un'altra queue). Tuttavia, potrebbero venire attivate inoltre le funzioni bash "duplex" e "tray", definite in `/usr/lib/lpdfilter/global/functions`, per permettere la stampa duplex o la scelta del cassetto dei fogli con comandi PostScript (a condizione che la stampante PostScript comprenda questi comandi)
- ▷ Se non vi è una stampante PostScript, Ghostscript verrà usato con un driver adatto al linguaggio del modello della stampante, per poter produrre dati che possano essere inviati alla stampante (o ad un'altra queue).
  Troverete i parametri per aprire Ghostscript in `/etc/printcap` direttamente nella riga `cm` o nel file `/etc/lpdfilter/`⟨*queue*⟩`/upp` (sostituite `queue` con il nome della queue).
  L'output di Ghostscript può essere anche riformattato, a condizione che `/etc/lpdfilter/`⟨*queue*⟩`/post` contenga uno script adatto (sostituite `queue` con il nome della queue).

(d) I dati di stampa vengono spediti alla stampante (o ad un'altra queue). Assieme ad essi, potete anche inviare sequenze di controllo specifiche, se impostate in `/etc/lpdfilter/`⟨*queue*⟩`/conf`.

Configurare lpdfilter

Normalmente il sistema di stampa viene configurato con YaST2 come descritto nella sezione *Configurare la stampante con YaST2* a pagina 61, e soprattutto viene configurato così anche il lpdfilter.

Per impostazioni speciali dovete adattare manualmente i file di configurazione del filtro della stampante.

Ogni queue ha il proprio file di configurazione `/etc/lpdfilter/`⟨*queue*⟩`/conf` (sostituite `queue` con il nome della queue) che contiene inoltre le informazioni su ogni opzione.

Completare individualmente il lpdfilter

1. Se i dati di stampa non sono PostScript, vengono trasformati in PostScript aprendo `/usr/lib/lpdfilter/filter/tipo2ps` laddove `tipo` sia da sostituirsi con il tipo di dati da stampare).

   Se sotto `/etc/lpdfilter/`⟨*queue*⟩`/`tipo2ps si trova uno script adatto, verrà anche utilizzato per tradurre i dati di stampa in PostScript. Questo script raccoglie i dati di stampa tramite `stdin` e li riproduce tramite `stdout` in formato PostScript.

2. I dati PostScript possono anche essere riformattati, a condizione che in `/etc/lpdfilter/`⟨*queue*⟩`/pre` vi sia uno script adatto. Potete aggiungere anche i vostri preload in formato PostScript, con lo script giusto. Questo script raccoglie i dati di stampa tramite `stdin` e li riproduce tramite `stdout` in formato PostScript. Applicazioni per riformattare dati PostScript, si trovano nel pacchetto `psutils`. In particolar modo pstops consente una riformattazione estesa; vedi a riguardo pagina di manuale di `pstops` (`man pstops`).

3. Parametri speciali per Ghostscript: durante la configurazione con YaST2, vengono memorizzati i parametri di chiamata di Ghostscript nel file `/etc/lpdfilter/`⟨*queue*⟩`/upp` (sostituite `queue` con il nome della queue). In questo file, potrete inserire manualmente anche dei parametri speciali per Ghostscript. Vd. anche il paragrafo *Su Ghostscript* a pagina 107.

4. Anche l'output di Ghostscript può essere riformattato, a condizione che sotto `/etc/lpdfilter/`⟨*queue*⟩`/post` vi sia uno script adatto (sostituite `queue` con il nome della queue). Questo script riceve l'output di Ghostscript tramite `stdin` e lo deve riprodurre nel formato adatto alla stampante tramite `stdout`.

Un esempio valido per tutti i tipi di hardware

Presupponendo che vi sia una queue `test`, nella quale debba essere stampato un testo ASCII con righe numerate e nella quale ogni foglio debba contenere due pagine ridotte. In questo caso, si possono creare i seguenti script: `/etc/lpdfilter/test/ascii2ps` ed `/etc/lpdfilter/test/pre`:

```
#!/bin/bash
cat -n - | a2ps -1 --stdin=' ' -o -
```

file 6: */etc/lpdfilter/test/ascii2ps: ASCII dopo la conversione in PostScript*

```
#!/bin/bash
pstops -q '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)'
```

file 7: */etc/lpdfilter/test/pre: Riformattazione PostScript*

Questi script devono poter essere eseguiti da ogni utente. Per far ciò, servitevi del comando `chmod`:

```
terra:~ #  chmod -v a+rx /etc/lpdfilter/test/ascii2ps
terra:~ #  chmod -v a+rx /etc/lpdfilter/test/pre
```

`pstops` funziona solo per file PostScript creati in modo da consentire la riformattazione (cosa che normalmente dovrebbe essere così).

Usare PostScript-preload individuali

I PostScript-Preload sono piccoli file PostScript che contengono comandi PostScript speciali e che vengono anteposti ai dati di stampa PostScript veri e propri, per inizializzare una stampante PostScript o Ghostscript con questi comandi speciali.

Normalmente, i PostScript-Preload vengono usati per attivare la stampa duplex su stampanti PostScript o per attivare cassetti di fogli speciali, oppure per impostare i margini e le correzioni gamma su stampanti PostScript o su Ghostscript.

L'importante è che la stampante PostScript o Ghostscript possano elaborare i comandi PostScript sotto descritti (Ghostscript non reagisce a comandi per stampa duplex o cassetto dei fogli). Supponiamo che la queue si chiami `test`.

Stampa duplex Per attivare e disattivare la stampa duplex, potete creare i seguenti file: `/etc/lpdfilter/test/duplexon.ps` e `/etc/lpdfilter/test/duplexoff.ps`:

```
%!PS
statusdict /setduplexmode known
{statusdict begin true setduplexmode end} if {} pop
```

file 8: */etc/lpdfilter/test/duplexon.ps: attivare stampa duplex*

```
%!PS
statusdict /setduplexmode known
{statusdict begin false setduplexmode end} if {} pop
```

file 9: */etc/lpdfilter/test/duplexoff.ps: disattivare stampa duplex*

Selezione del cassetto della carta Per attivare il cassetto della carta standard con la cifra 0 o il cassetto per esempio con la cifra 2, potete creare i seguenti file `/etc/lpdfilter/test/tray0.ps` e `/etc/lpdfilter/test/tray2.ps`:

```
%!PS
statusdict /setpapertray known
{statusdict begin 0 setpapertray end} if {} pop
```

file 10: */etc/lpdfilter/test/tray0.ps: attivare cassetto 0*

```
%!PS
statusdict /setpapertray known
{statusdict begin 2 setpapertray end} if {} pop
```

file 11: */etc/lpdfilter/test/tray2.ps: attivare cassetto 2*

Margini Per modificare i margini, potete creare il seguente file `/etc/lpdfilter/test/margin.ps`:

```
%!PS
<<
/.HWMargins [left bottom right top]
/PageSize [width height]
/Margins [left-offset top-offset]
>>
setpagedevice
```

file 12: */etc/lpdfilter/test/margin.ps: margini*

Le impostazioni dei margini `left`, `bottom`, `right` e `top` e le dimensioni del foglio `width` e `height` sono espressi in punti (laddove un punto corrisponde a 1/72 pollici o circa 0.35 mm). Gli offset `left-offset` e `top-offset` sono in punti di matrice e dipendono quindi dalla risoluzione.

Per spostare la posizione della stampa sul foglio, basta il file `/etc/lpdfilter/test/offset.ps`

```
%!PS
<< /Margins [left-offset top-offset] >> setpagedevice
```

file 13: */etc/lpdfilter/test/offset.ps: Posizione del stampato*

Correzioni gamma Per modificare la distribuzione della luminosità dei colori, create i file `/etc/lpdfilter/test/cmyk.ps` ed `/etc/lpdfilter/test/rgb.ps`:

```
%!PS
{cyan exp} {magenta exp} {yellow exp} {black exp} setcolortransfer
```

file 14: */etc/lpdfilter/test/cmyk.ps: correzione gamma CMYK*

```
%!PS
\{red exp\} \{green exp\} \{blue exp\} currenttransfer setcolortransfer
```

file 15: */etc/lpdfilter/test/rgb.ps: correzione gamma RGB*

Il modello di colore (CMYK o RGB) deve adattarsi alla vostra stampante. I valori da impostare per `cyan`, `magenta`, `yellow`, `black`, `red`, `green` e `blue`, possono essere determinati a seguito di test. Comunque dovranno essere tra `0.001` e `0.999`.

Potete verificare l'effetto dei file sopra descritti con l'interfaccia grafica, sullo schermo, senza correzioni gamma:

```
terra:~ #  gs -r60 \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Con correzioni gamma di uno di questi esempi:

```
terra:~ #  gs -r60 /etc/lpdfilter/test/cmyk.ps \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps
terra:~ #  gs -r60 /etc/lpdfilter/test/rgb.ps \
    /usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Il comando va inserito su una sola riga e senza (ingl. *Backslash,* \).

Per chiudere, premere Ctrl + C.

Resettare la stampante Per riportare la stampante alle impostazioni di default, potete creare il seguente file `/etc/lpdfilter/test/reset.ps`:

```
%!PS
serverdict begin 0 exitserver
```

file 16: */etc/lpdfilter/test/reset.ps: resettare la stampante*

Per attivare un file PostScript-preload, potete creare il seguente script `/etc/lpdfilter/test/pre`:

```
#!/bin/bash
cat /etc/lpdfilter/test/preload.ps -
```

file 17: */etc/lpdfilter/test/pre: caricare PostScript-Preload*

Sostituite `preload` con il nome del file preload adatto. Lo script deve essere eseguibile e leggibile per tutti gli utenti viene realizzato con il comando `chmod`:

```
terra:~ #  chmod -v a+rx /etc/lpdfilter/test/pre
terra:~ #  chmod -v a+r /etc/lpdfilter/test/preload.ps
```

Potete usare lo stesso meccanismo per inviare un file PostScript alla stampante non solo prima, ma anche dopo i veri e propri dati di stampa PostScript. Ad esempio, per resettare la stampante alla fine di una stampa, potete creare il seguente script `/etc/lpdfilter/test/pre`:

```
%

#!/bin/bash
cat /etc/lpdfilter/test/preload.ps - /etc/lpdfilter/test/reset.ps
```

file 18: */etc/lpdfilter/test/pre: PostScript-Preload e PostScript-Reset*

Esempio di configurazione di una stampante cosìddetta GDI

Vogliamo ora configurare una queue `gdi` per una stampante GDI

Questo tipo di stampanti normalmente non può essere usato con Linux, vd. paragrafo precedente *La stampante GDI*.

Tuttavia esistono per alcune stampanti GDI speciali programmi driver che normalmente vengono utilizzati come complemento a Ghostscript, convertendo l'output di Ghostscript nel formato adatto alla stampante. Questo tipo di programmi driver comportano spesso molte restrizioni per quanto riguarda la stampa – per esempio stampano solo in bianco e nero.

Ghostscript e i programmi driver si complementano come segue (cfr. il paragrafo *Su Ghostscript*)

1. I dati PostScript vengono risolti da Ghostscript in una matrice di tanti punti. I dati della matrice vengono poi riprodotti, tramite un programma driver collegato in serie adatto al driver Ghostscript, ed emessi nel formato giusto e con la risoluzione giusta.
2. I dati della matrice vengono convertiti nel formato della stampante attraverso il programma driver.

Si parte qui dal presupposto che disponete di un programma driver per la stampante adatto alla vostra versione di SuSE Linux Enterprise Server o che possa essere scaricato dall'Internet. Si presuppone anche il programma driver funzioni come descritto sopra, e che voi sappiate usare Unix (per esempio con archivi `.zip` o `.tar.gz` oppure pacchetti `.rpm`). Dopo aver decompresso un tale archivio, troverete delle istruzioni all'installazione in file di nome `README` o `INSTALL` o in una sottodirectory di nome `doc`. Nel caso degli archivi `.tar.gz`, il programma driver vero e proprio deve essere compilato ed installato.

Di seguito, presupporremo anche che:

- il programma driver sia `/usr/local/bin/printerdriver`.
- il driver Ghostscript serva `pbmraw` con una risoluzione di 600 dpi.
- la stampante sia collegata alla prima interfaccia parallela `/dev/lp0`.

Quale driver Ghostscript e quale risoluzione utilizzare effettivamente viene indicato nella documentazione del programma driver Per prima cosa, create la queue `gdi` con lprsetup (come `root`):

```
terra:~ #  lprsetup -add gdi -lprng -device /dev/lp0 \
     -driver pbmraw -dpi 600 -size a4dj -auto -sf
```

Questo comando va scritto in una sola riga senza backslash, '`\`'.

Quindi, generate il seguente script `/etc/lpdfilter/gdi/post`:

```
#!/bin/bash
/usr/local/bin/printerdriver ⟨parametri_specifici-del-driver⟩
```

file 19: */etc/lpdfilter/gdi/post: chiamata del programma di driver*

Eventualmente inserire i ⟨*parametri_specifici-del-driver*⟩ adatti. Quali parametri specifici del driver utilizzare effettivamente viene indicato nella documentazione del programma driver.

Lo script deve poter essere eseguito da tutti gli utenti; infine, riavviare in seguito lo spooler:

```
terra:~ #  chmod -v a+rx /etc/lpdfilter/gdi/post
terra:~ #  rclpd stop
terra:~ #  rclpd start
```

Ora, tutti gli utenti potranno stampare come segue:

```
tux@terra:~ >  lpr -Pgdi ⟨file⟩
```

Ricerca degli errori nel lpdfilter

Per attivare il debug-level giusto, eliminate il simbolo di commento # davanti alla riga corrispondente nello script principale `/usr/lib/lpdfilter/bin/if` del filtro della stampante.

```
# DEBUG="off"
# DEBUG="low"
DEBUG="medium"
# DEBUG="high"
```

file 20: */usr/lib/lpdfilter/bin/if: livello di debug*

Con `DEBUG=low`, verranno salvati solo gli output `stderr` di `/usr/lib/lpdfilter/bin/if` in un file `/tmp/lpdfilter.if-$$.XXXXXX` (sostituite a `$$` il numero del processo; a `XXXXXX` sostituite una combinazione di cifre casuale ma univoca).

Con `DEBUG=medium`, vengono salvati anche gli output `stderr` degli script sotto `/usr/lib/lpdfilter/filter/` che vengono caricati con `/usr/lib/lpdfilter/bin/if`. Essi vengono memorizzati in file del tipo `/tmp/lpdfilter.nome-$$.XXXXXX` (laddove `nome` sia il nome dello script caricato e `$$.XXXXXX` una combinazione di cifre casuale ma univoca).

Con `DEBUG=high`, l'output non viene inviato alla stampante, ma memorizzato in un file del tipo `/tmp/lpdfilter.out-$$.XXXXXX` (dove `$$.XXXXXX` sia una combinazione di cifre casuale ma univoca).

Per mantenere un pò d'ordine, cancellate questi file prima di ogni test con `rm -v /tmp/lpdfilter*`.

Generare propri filtri di stampante per lo spooler della stampante

Premesse

Lo scopo di questa sezione, non è quello di presentare un'alternativa a lpdfilter, ma di spiegare i retroscena della stampa sotto Linux in base a un esempio di filtro per stampante creato individualmente. Per poter spiegare con chiarezza i passi più importanti, riportiamo un esempio semplice. Per questo si è rinunciato anche ad una descrizione del modo per eliminare degli errori nello script del filtro.

In seguito, si parte dal presupposto che la stampante sia collegata alla prima interfaccia parallela `/dev/lp0`.

Un filtro riceve, attraverso lo spooler, i dati da stampare tramite l'immissione standard. Il filtro della stampante deve trasformare questi dati nel formato della stampante ed emetterli tramite l'emissione standard. Lo spooler procura che tutto ciò che viene emesso dal filtro tramite l'emissione standard, arrivi al dispsitivo della stampante `/dev/lp0`. Il kernel da parte sua inoltra all'interfaccia da definire (p.e. all'indirizzo IO `0x378`) tutto quello che arriva al device della stampante. L'hardware provvede che tutto quello che viene per esempio mandato all'indirizzo IO `0x378`, venga inviato attraverso l'interfaccia parallela. La stampante interpreta questo flusso di dati e li stampa.

Normalmente, i seguenti comandi possono solo venire eseguiti come utente `root`; questo perché i "normali" utenti non possono accedere direttamente al dispositivo della stampante.

comandi vengano indicati come segue:

```
terra:~ #  cat file ascii >/dev/lp0
```

Sia ben chiaro che `cat file ascii` deve venire sostituito con il nome di un file ASCII esistente.

Un semplice esempio sul metodo fondamentale di lavoro

Tramite il comando

```
terra:~ #  echo -en "\rHello\r\f" >/dev/lp0
```

non viene attivato alcun spooler o filtro della stampante, poiché viene direttamente indirizzato il device della stampante `/dev/lp0`. In questo modo, solo i caratteri ASCII `'\r'`, `'H'`, `'e'`, `'l'`, `'o'` e `'\r'` e `'\f'` vengono subito inviati alla stampante. Il carattere FormFeed-ASCII `'\r'` sta per un capoverso e `'\f'` provoca un avanzamento di modulo nella stampante

Con

```
terra:~ #  cat ascii-file >/dev/lp0
terra:~ #  echo -en "\f" >/dev/lp0
```

non vengono attivati né lo spooler né il filtro della stampante, poiché viene indirizzato direttamente il device della stampante `/dev/lp0`. I caratteri ASCII del file di testo ASCII, vengono inviati direttamente alla stampante ed infine un carattere Form Feed ASCII per emettere l'ulitima pagina dalla stampante.

Sotto Linux, due righe di testo ASCII vengono divise solo da un carattere interlinea-ASCII (ingl. *line feed*); sotto DOS/Windows due righe di testo ASCII vengono separate da un carattere LineFeed-ASCII e da un carattere CarriageReturn (ritorno carrello).

Se con il suddetto comando si invia direttamente alla stampante un file di testo ASCII, si ha normalmente questa sequenza

```
terra:~ #  cat /etc/SuSE-release >/dev/lp0
terra:~ #  echo -en "\f" >/dev/lp0


SuSE Linux 8.1 (i386)
                     VERSION = 8.1
```

poiché la stampante esegue solo un line feed, ma non esegue il ritorno di carrello in quanto non vi è alcun carattere CarriageReturn-ASCII.

È però possibile impostare la stampante in modo che questa, con un carattere LineFeed-ASCII esegua sia un'interlinea che un ritorno carrello (ingl. *carriage return*).

Con la sequenza escape `\033&k2G`, le stampanti che capiscono la lingua PCL 3 vengono impostate in modo che con un carattere LineFeed-ASCII venga eseguita un'interlinea e un ritorno carrello. Con

```
terra:~ #  echo -en "\033&k2G" >/dev/lp0
```

la sequenza escape viene inviata alla stampante e alla fine viene stampato il file di testo ASCII con l'interlinea giusta.

Probabilmente, gli accenti non verranno stampati correttamente, perché su DOS/Windows la codificazione degli accenti è diversa da Linux e la stampante è normalmente preimpostata per DOS/Windows.

Con

```
terra:~ #  cp ascii-file ascii-file.ibmpc
terra:~ #  recode lat1..ibmpc ascii-file.ibmpc
```

viene prima copiato il file di testo ascii nel file di testo ascii.ibmpc e quindi `ascii-file.ibmpc` viene ricodificato per DOS/Windows.

Con

```
terra:~ #  cat ascii-file.ibmpc >/dev/lp0
terra:~ #  echo -en "\f" >/dev/lp0
```

dovrebbero venir stampati correttamente sia le interlinee che gli accenti. Poiché nel file `ascii-file.ibmpc` sia l'interlinea che gli accenti sono codificati secondo DOS/Windows, non è più necessaria alcuna speciale sequenza escape per impostare nella stampante l'interlinea adatta.

Dunque con

```
terra:~ #  cp ascii-file ascii-file.ibmpc
terra:~ #  recode lat1..ibmpc ascii-file.ibmpc
terra:~ #  cat ascii-file.ibmpc >/dev/lp0
terra:~ #  echo -en "\f" >/dev/lp0
```

dovrebbe quindi essere possibile stampare correttamente qualsiasi file di testo ASCII su ogni stampante idonea a stampare un testo ASCII e ad usare i caratteri DOS/Windows.

Se ciò funziona, è ovvio creare un filtro per la stampante che esegua automaticamente la conversione del file di testo ASCII nel formato specifico della stampante.

Esempio di filtro della stampante generato in proprio

Innanzitutto, creeremo una sottodirectory per il filtro e la apriremo come `root`):

```
terra:~ #  mkdir /usr/local/il-mio-filtro-della-stampante
terra:~ #  cd /usr/local/il-mio-filtro-della-stampante
```

Create uno script bash (come file di testo ASCII) con il nome `asciifilter`, come elencato nel file a fronte 21.

```
#!/bin/bash

# make a temporary file
INPUT="$(mktemp /tmp/asciifilter.$$.XXXXXX)"

# First store everything from stdin in $INPUT
# to have the input as a regular file
cat >$INPUT

# Recode the INPUT
recode lat1..ibmpc $INPUT

# Add a FormFeed at the end of $INPUT
# to get the last page out of the printer
echo -en "\f" >>$INPUT

# Send $INPUT to stdout
cat $INPUT

# Remove the INPUT file
rm $INPUT
```

file 21: */usr/local/myprinterfilter/asciifilter*

Rendete questo script eseguibile da ogni utente con

```
terra:~ #  chmod -v a+x /usr/local/myprinterfilter/
terra:~ #  chmod -v a+rx /usr/local/myprinterfilter/asciifilter
```

Con `lprsetup` create una queue supplementare (vd. `lprsetup --help`). Denominatela, in questo caso, `af` (ovvero “asciifilter”).

```
terra:~ #  lprsetup -add af -lprng -device /dev/lp0 -raw -sf
```

Sostituite, per il valore `af` in `/etc/printcap`, nella riga `if`, solo `/usr/lib/lpdfilter/bin/if` con `/usr/local/il-mio-filtro-della-stampante/asciifilter`, in modo che la registrazione `af` sia come segue:

```
af:\
        :cm=lpdfilter drv= method=raw color=no:\
        :lp=/dev/lp0:\
        :sd=/var/spool/lpd/af:\
        :lf=/var/spool/lpd/af/log:\
        :af=/var/spool/lpd/af/acct:\
        :if=/usr/local/myprinterfilter/asciifilter:\
        :la@:mx#0:\
        :tr=:cl:sh:
```

file 22: */etc/printcap: filtro proprio*

Fermate e riavviate lo spooler della stampante con

```
terra:~ #  rclpd stop
terra:~ #  rclpd start
```

Ora, tutti gli utenti dovrebbero essere in grado di stampare tramite la nuova queue af, con il comando

```
tux@terra:~ >  lpr -Paf file ascii
```

Il sistema di stampante CUPS

Terminologia

Con “client” o “programma client” si indica un programma che viene inizializzato per inviare degli incarichi da stampare al demone CUPS.

Un “demone” è un servizio locale che riceve gli incarichi da stampare e li inoltra o li elaborare.

Un “server” è un demone che fornisce a una o più stampante i dati da stampare. Ogni server ha contemporaneamente la funzione di un demone.

Di solito non viene differenziato né da coloro che usano CUPS né dagli sviluppatori di CUPS tra i termini “server” e “demone”.

IPP e server

Gli incarichi da stampare vengono inviati con programmi basati su CUPS come `lpr`, `kprinter` o `xpp`, e tramite l’ *Internet Printing Protocols*, abbreviato con IPP ed è definito negli “standard Internet” RFC-2910 e RFC-2911 (vd.

http://www.rfc-editor.org/rfc.html). L' IPP è un protocollo Web simile a HTTP: gli stessi header, ma diversi dati utente. Viene utilizzate anche un'altra, propria porta 631 ai fini della comunicazione, registrato comunque dalla IANA (ingl. *Internet Authority for Number Allocation*).

I dati vengono inviati al demone CUPS configurato, che normalmente è anche il server locale. Altri demoni per esempio possono essere indirizzati direttamente tramite la variabile shell CUPS_SERVER .

Con la funzione "broadcast" del demone CUPS, le stampanti locali gestiti dallo stesso demone possono essere rese note nella rete (UDP Porta 631) e appaiono come queue ai demoni che ricevono/analizzano questi pacchetti broadcast (configurabili). Questo è un vantaggio per reti aziendali, perché permette di "vedere", dopo l'avvio del computer, tutte le stampanti a disposizione, senza dover configurare manualmente alcunché. Questo comunque comporta un rischio quando il computer è collegato ad Internet. Nella configurazione con la funzionalità broadcast dovete far sì che il broadcast si propaghi solo all'interno della rete locale, che l'accesso sia permesso solo per la rete locale e che l'indirizzo IP pubblico per la connessione ad Internet non si trovi nell'area degli indirizzi della rete locale, altrimenti anche altri utenti dello stesso ISP potrebbero "vedere" le stampanti che vengono rese note dal broadcast e utilizzarle. Inoltre i broadcast generano traffico di rete che può comportare dei costi aggiuntivi. Per tale ragione bisogna sempre assicurare che i pacchetti broadcast non vengano inviati dalla stampante locale nell'Internet, per esempio con il firewall di SuSE che filtra i pacchetti. Per ricevere degli broadcast non si deve configurare in aggiunta alcunché. Solo all'invio deve venire indicato un indirizzo broadcast (per esempio configurare tramite YaST2).

L'IPP viene utilizzato per la comunizione tra demoni CUPS locale e remoti (dunque un server CUPS). Le moderni stampanti di rete supportano adesso anche l'IPP. Ulteriori informazioni si trovano sulle pagine Web della casa produttrice o nel manuale delle stampante.

Windows 2000 e successivi offrono anche il supporto IPP. Purtroppo vi sono state delle difficoltà con il formato di implementazione di Windows. Probabilmente questi problemi sono stati superati o possono essere eliminati con il service pack.

Configurazione del server CUPS

Vi sono tanti modi per configurare delle stampanti sotto CUPS e di configurare il demone: con tools a riga di comando, YaST2, Centro di controllo di KDE, interfaccia Web etc. Nei paragrafi che seguono verranno trattati solo i

tool a riga di comando e YaST2. Comunque, ripetiamo che queste non sono le uniche possibilità.

Attenzione

L'interfaccia Web comporta il rischio di compromettere la password di root, poiché è possibile inviare tramite rete la password in forma non cifrata appena nell'URL viene immesso il nome del computer. Per tale ragione si consiglia assolutamente di usare solo `http://localhost:631/` e nessun altro indirizzo.

Attenzione

Ed è anche per questo motivo che l'accesso ai fini amministrativi ai demoni CUPS è stato ristretto in modo che può essere configurato solo indirizzato con "localhost" (che è identico all'indirizzo IP `127.0.0.1`.) Altrimenti appare un messaggio di errore.

Per amministrare stampanti locali è necessario che un demone CUPS giri su di un computer locale. A tal fine si deve installare il pacchetto `cups` e i file PPD generati da SuSE nei pacchetti `cups-drivers` e `cups-drivers-stp`. Poi si lancia il server (come `root`) con il comando: `/etc/rc.d/cups restart`. Nel processo di configurazione con YaST2 l' installazione e l'avvio avviene implicitamente selezionando CUPS quale sistema di stampa e all'installazione della stampante.

PPD sta per "PostScript Printer Description" ed è uno standard per descrivere le opzioni della stampante con comandi PostScript. Esse sono necessari in CUPS per installare stampanti. SuSE Linux fornisce file PPD generati per numerosi stampanti di diverse case produttrice. Comunque anche le case progruttici mettono a disposizione su Internet e CD di installazione file PPD per stampanti (soprattutto nel settore "installazione sotto Windows NT").

Il demone locale può essere lanciato per avere a disposizione localmente tutte le stampanti di tutti i server broadcast, senza disporre localmente di una sola stampante, cioè per la selezionare la stampante sotto KDE e OpenOffice nel modo meno laborioso possibile.

Il broadcast si configura con YaST2, o nel file `/etc/cups/cupsd.conf` si può impostare la variabile "Browsing" su `On` (default) e la variabile "BrowseAddress" su un valore adatto (per esempio `192.168.255.255`). Per la ricezione degli incarichi di stampa, dovete almeno premettere a `<Location /printers>`, o meglio a `<Location />` di prenderli in consegna. Dovete completare `Allow From xyz-host.mydomain` – vedi `file:/usr/share/doc/packages/cups/sam.html`. Con il comando `/etc/rc.d/cups reload` (come root) viene applicata, dopo aver editato il file del demone, la nuova configurazione.

Stampante di rete

Una stampante di rete è un stampante con un'interfaccia di rete per il server della stampante (come il caso di HP con il JetDirect Interface) o stampanti colleganti ad una box di server della stampa o box router con funzionalità di server della stampante o qualcosa di paragonabile. Non si intende in questo caso computer Windows che mettono la stampante a disposizione come "share". Comunque anche sotto CUPS anche questo tipo di stampante è facilmente indirizzabile in modo simile.

Stampanti di rete supportano nella maggior parte dei casi il protocollo LPD (su porta 515). Potete controllarlo con il seguente comando:

```
netcat -z nome-del-computer.dominio 515 && echo ok || echo failed
```

Allora si possono configurare con l'URI del dispositivo (terminologia di CUPS) `lpd://Server/Queue`. Per ulteriori dettagli a riguardo `file:/usr/share/doc/packages/cups/sam.html`.

Di solito è preferibile indirizzare queste stampanti tramite la porta 9100 (HP, Kyocera e tanti altri) integrata o la porta 35 (QMS), cioè senza frapporre un protocollo LPD. L'URI del dispositivo è `socket://Server:Port/`

Per stampare con stampanti Windows deve essere installato il pacchetto `samba-client` e Samba deve essere configurato in modo corretto, cioè deve essere impostato il giusto "workgroup", etc. L'URI del dispositivo per computer che girano su Windows può essere composta in modo diverso. Spesso comunque sarà: `smb://user:password@host/printer`. Per tutte le altre possibilità vedi `file:/usr/share/doc/packages/cups/sam.html` e la pagina di manuale di `smbspool` (`man smbspool`).

Dopo aver configurato la stampante di rete e si ha una piccola rete con diversi PC (Linux), sarebbe comodo non dover configurare la stampante di rete su ogni client. Così va attivata la funzionalità "Broadcast" del demone (vd. sopra.). Non è necessario neanche modificare la configurazione, p.e. dimensione standard dei fogli su `Letter` su ogni singolo client, basta farlo una volta sul server (vd. sezione *Impostazione della queue* a pagina 105). Questi interventi vengono salvati localmente, però valgono anche per i client grazie ai tool CUPS, o meglio a causa del protocollo IPP.

Elaborazione interna dell'incarico

Conversione in PostScript

In linea di massima ogni tipo di file può essere inviato ad un demone CUPS. I file PostScript comunque in questo caso non creano alcuna difficoltà. La conversione in PostScript attraverso CUPS avviene dopo che il tipo di file è

stato identificato sulla base di `/etc/cups/mime.types` e di seguito viene richiamato il corrispondente tool che si trova in `/etc/cups/mime.convs`. Il processo di conversione si differenzia da spooler LPR tradizionali per il fatto che avviene sul server e non sul client. Lo scopo era quello di eseguire la conversione solo sul server preposto alla stampante, il che comporta sia dei vantaggi che svantaggi.

Conteggio

Dopo la conversione in PostScript, viene determintato il numero di pagine dell'incarico da stampare. A tal fine CUPS lancia il (proprio) tool pstops (`/usr/lib/cups/filter/pstops`). Il numero di pagine dell'incarico viene scritto successivamente su `/var/log/cups/page_log`.

Le registrazioni sono:

- Nome della stampante (p.e. `lp`),
- Nome dell'utente (p.e. `root`),
- Numero dell'incarico,
- Data nella parentesi quadra [],
- Il numero della pagina in fase di stampa,
- Numero delle copie.

Ulteriori filtri di conversione

Inoltre potete attivare altri filtri, previa selezione delle corrispondenti opzioni per la stampa. Di particolare interesse sono i seguenti:

psselect: per stampare solo certe pagine del documento,

ps-n-up: per stampare più pagine del documento su un foglio.

Questi filtri non possono essere configurati. Come attivare le opzioni viene descritto in `file:/usr/share/doc/packages/cups/sum.html`.

Conversione specifica per la stampante

Adesso avviamo il filtro necessario per generare dati specifici da stampare (per esempio `/usr/lib/cups/filter/cupsomatic`). Questo filtro può essere indicato nel file PPD di installazione, altrimenti si parte dal presupposto che si dispone di una stampante PostScript. Tutte le opzioni che dipendono dal dispositivo, come risoluzione e dimensione dei fogli, vengono elaborati in questo filtro.

Non è facile e dunque non è consigliabile compilare filtri specifici per stampanti propri.

Emissione al dispositivo di stampa

Infine viene richiamato il back-end. Si tratta di un filtro speciale che emette i dati da stampare servendosi di un dispositivo o una stampante di rete (vd. `/usr/share/doc/packages/cups/overview.html`). Il back-end consente di comunicare con il dispositivo o la stampante di rete (dipende dall'URI del dispositivo indicato durante l'installazione). Un back-end può essere per esempio `usb`, in questo caso verrebbe lanciato il programma `/usr/lib/cups/backend/usb`, ove il dispositivo USB verrebbe aperto, bloccato e pre-inizializzato nel filesystem, e i dati provenienti dal filtro verrebbero inoltrati. Alla fine, il dispositivo viene disinizializzato e messo a disposizione nel sistema.

Attualmente esistono back-end paralleli, seriali, usb, ipp, lpd, http, socket (dal pacchetto CUPS), ed inoltre canon e epson (da `cups-drivers-stp`), e smb (da `samba-client`).

Senza filtro

Se si vuole stampare senza alcun filtro si può scegliere l'opzione `-l` accanto al comando `lpr`, oppure `-oraw` accanto a `lp`. Normalmente le stampanti non funzionano, poiché non lanciano GhostScript che funge da interprete. (cupsomatic) o altri filtri importanti. Nel caso di tool CUPS le opzioni hanno nomi simili.

Suggerimento

OpenOffice

Se stampate su OpenOffice con CUPS, non dovete più, come era il caso con StarOffice 5.2, configurare le stampanti una a una. OpenOffice le "riconosce" ora, se gira un demone CUPS e gli chiede quali sono le stampanti e le

opzioni esistenti. In futuro non dovrebbe essere più necessario configurare ulteriormente OpenOffice.

Se si vogliono usare propri tool CUPS per stampare sotto OpenOffice, si dovrebbe evitare di richiamare un programma come comando di stampa che visualizza anche finestre di dialogo; `kprinter` o `xpp` ne sono un esempio. Questi programmi possono causare un blocco di OpenOffice mentre sono attivi dei processi.

Windows

Le stampanti collegati ad un computer con Windows possono essere indirizzati con l'URI del dispositivo `smb://server/printer` – vedi soprap.

Nel caso inverso, si vuole stampare con Windows servendosi di un server CUPS, nel file di configurazione Samba `/etc/samba/smb.conf` deve venir impostata la registrazione `printing = cups` o `printing = CUPS` e riavviare il server smb – vedi anche `file:/usr/share/doc/packages/cups/sam.html`

Stampante Raw

Si può configurare una stampante Raw ommettendo il file PPD durante l'installazione, cioè non vi sarà né filtraggio né conteggio. I dati devono essere inviati nel formato della stampante. Dei test eseguiti da SuSE non sempre hanno portato al risultato desiderato, per questo al momento non consigliamo questo metodo.

Opzioni della stampante propri

Le opzioni di configurazione (per esempio di solito altro numero DPI) vengono memorizzati nel file `~/.lpoptions`. Se una stampante "riconfigurata" viene staccata dal server, rimane visibile nei diversi tool, come `kprinter` o `xpp`. Anche se non esiste più, può essere selezionata, cosa che chiaramente comporta dei problemi. Utenti più esperti sapranno cancellare le righe imputate senza difficoltà alcuna da `~/.lpoptions` servendosi di un editor.

Compatibilità con LPR

CUPS può anche ricevere incarichi da sistemi LPR. Le impostazioni necessari in `/etc/inetd.conf` possono essere eseguiti con YaST2, oppure va eliminato il simbolo di commento all'inizio della riga "printer" in `/etc/inetd.conf`. Per esempio (come `root`) con:

```
perl -pi -e 's:^\# (printer):$1:' /etc/inetd.conf
rcinetd reload
```

Se si vuole tornare su LPRng alla riga va preposto nuovamente il simbolo di commento:

```
perl -pi -e 's:^(printer):# $1:' /etc/inetd.conf
rcinetd reload
```

Tool della riga di comando per il sistema di stampa CUPS

I tool della riga di comando e le relative pagine di manuale per il sistema di stampa CUPS si trovano nel pacchetto `cups-client` e la documentazione è reperibile nel pacchetto `cups` sotto `/usr/share/doc/packages/cups/` i particolar modo il "CUPS Software Users Manual" sotto
`file:/usr/share/doc/packages/cups/sum.html`
e il "CUPS Software Administrators Manual" sotto
`file:/usr/share/doc/packages/cups/sam.html`
che con cupsd in esecuzione localmente si trova anche sotto
`http://localhost:631/documentation.html`
Nel caso dei tool della riga comando CUPS a volte è determinante l'ordine delle opzioni. In caso di dubbi consultate la relativa pagina di manuale.

Per queue locali

Generare incarichi di stampa

Di solito si preme su "System V Art" con

`tux@terra:~ >` **`lp -d`** ⟨***`queue`***⟩ ⟨***`file`***⟩

o su "Berkeley Art" con

`tux@terra:~ >` **`lpr -P`**⟨***`queue`***⟩ ⟨***`file`***⟩

ulteriori informazioni nella pagina di manuale di `lpr` (`man lpr`) e pagina di manuale di `lp` (`man lp`) nonché nella sezione "Using the Printing System" sotto
`file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM`
nel *CUPS Software Users Manual*.

Con il parametro addizionale `-o` possono essere stabilite opzioni di ampia portata relative al tipo del stampato. Ulteriori informazioni nella pagina di manuale di `lpr` (`man lpr`) e pagina di manuale di `lp` (`man lp`) nonché nella sezione "Standard Printer Options" sotto
`file:/usr/share/doc/packages/cups/sum.html#STANDARD_OPTIONS`
nel *CUPS Software Users Manual*.

Visualizzare lo stato

Lo stato della queue viene indcato su "System V Art" con

```
tux@terra:~ >  lpstat -o ⟨queue⟩ -p ⟨queue⟩
```

o su "Berkeley Art" con

```
tux@terra:~ >  lpq -P⟨queue⟩
```

Senza la indicazione di una queue, verranno indicate tutte le queue, laddove `lpstat -o` indicat tutti gli incarichi attivi nella forma di ⟨*queue*⟩-⟨*numero dell'incarico*⟩.

Con `lpstat -l -o` ⟨*queue*⟩ `-p` ⟨*queue*⟩ vengono indicati più informazioni e con `lpstat -t lpstat -l -t` viene indicate il massimo di informazione disponibile.

Ulteriori informazioni nella pagina di manuale di `lpq` (`man lpq`), nella pagina di manuale di `lpstat` (`man lpstat`) e nella sezione "Using the Printing System" sotto
`file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM`
nel *CUPS Software Users Manual*.

Cancellare incarichi di stampa

Su "tipo System V"

```
tux@terra:~ >  cancel ⟨queue⟩-⟨numero dell'incarico⟩
```

o su "tipo Berkeley Art"

```
tux@terra:~ >  lprm -P⟨queue⟩ ⟨numero dell'incarico⟩
```

cancella l'incarico dalla queue indicata con il numero dell'incarico indicato.

Ulteriori informazioni nella pagina di manuale di `lprm` (`man lprm`) e nella pagina di manuale di `cancel` (`man cancel`) e nella sezione "Using the Printing System" sotto
`file:/usr/share/doc/packages/cups/sum.html#USING_SYSTEM`
nel *CUPS Software Users Manual*.

Impostazione della queue

Nel *CUPS Software Users Manual* nella sezione “Standard Printer Options” sotto
`file:/usr/share/doc/packages/cups/sum.html#STANDARD_OPTIONS`
vengono descritte opzioni standard indipendenti dall’hardware per il tipo dello stampanto e nella sezione “Saving Printer Options and Defaults” sotto
`file:/usr/share/doc/packages/cups/sum.html#SAVING_OPTIONS`
viene descritto come salvare le impostazioni delle opzioni.

Le opzioni specifiche della stampante per il tipo dello stampato sono stabiliti nel file PPD appartenente alla corrispondente queue e vengono indicati con il comando

```
tux@terra:~ >  lpoptions -p ⟨queue⟩ -l
```

nella forma seguente:

```
Option/Text: valore valore valore ...
```

chiaramente un * davanti al valore della opzione caratterizza l’impostazione attuale.

Esempio:

```
PageSize/Page Size: A3 *A4 A5 Legal Letter
Resolution/Resolution: 150 *300 600
```

Nell’esempio opzione `PageSize` è impostata su `A4` e la risoluzione sul valore `300`.

Con

```
tux@terra:~ >  lpoptions -p ⟨queue⟩ -o opzione=valore
```

può essere impostato un valore diverso.

Nell’esempio di sopra con

```
tux@terra:~ >  lpoptions -p ⟨queue⟩ -o PageSize=Letter
```

la dimensione della carta viene impostata su `Letter` per la queue corrispondente.

Se un utente normale immette il comando `lpoptions`, le impostazioni vengono salvate solo per questo utente nel file `~/.lpoptions`.

Se l'amministratore di sistema `root` immette il comando `lpoptions`, le impostazioni vengono salvati nel file `/etc/cups/lpoptions` come impostazione di default per tutti gli utenti sul computer locale. Il file PPD non viene modificato.

Solo se si modificano le impostazioni di default nel file PPD di una queue, esse saranno valide per tutti gli utenti nella rete che si servono di questa queue per stampare.

L'amministratore del sistema può modificare le impostazioni di default nel file PPD di una queue con

```
terra:~ #  lpadmin -p ⟨queue⟩ -o opzione=valore
```

così nell'esempio di sopra con

```
terra:~ #  lpadmin -p ⟨queue⟩ -o PageSize=Letter
```

viene cambiata la dimensione dei fogli di default su `Letter` per la corrispondente queue per tutti gli utenti nella rete.

Queue remote

`server della stampate` viene sostituito con il nome o l'indirizzo IP del server della stampante e ⟨*queue*⟩ deve essere una queue sul server della stampante.

Qui vengono indicati solo i comandi principali. Per quanto rigurda ulteriori possibilità e fonte di informazioni vedi la sezione *Per queue locali* a pagina 103.

Generare incarichi di stampa

Su " tipo System V " con

```
tux@terra:~ >  lp -d ⟨queue⟩ -h server-della-stampante ⟨file⟩
```

o su "tipo Berkeley" con

```
tux@terra:~ >  lpr -P⟨queue⟩@server-della-stampante ⟨file⟩
```

si genera l'incarico sul server della stampante indicato nella queue indicata.

Premessa: il server della stampante è configurato in modo che si ha il permesso di stampare servendosi delle sue queue. Di default questo non è possibile con CUPS, ma con la configurazione della stampante di YaST2, in un ramo del menu esteso, si ha la possibilità di modificare le impostazione per il server CUPS.

Visualizzare lo stato

Su “tipo System V” con

```
tux@terra:~ >  lpstat -h server della stampante -o ⟨queue⟩ -p
     ⟨queue⟩
```

viene visualizzato lo stato di una queue sul server della stampante.

Cancellare incarichi di stampa

Il comando “tipo System V”

```
tux@terra:~ >  cancel -h server della stampante ⟨queue⟩-⟨numero
     dell'incarico⟩
```

cancella l'incarico con il numero d'incarico indicato dalla queue indicata sul server della stampante.

Eliminare disfunzioni con il comando di sopra in CUPS

Si procede in modo analogo alla sezione *Eliminare disfunzioni con il comando descritto sopra in LPRng* a pagina 82, con la sola differenza che con CUPS nella seconda parte si devono immmettere altri comandi:

1. Togliete la carta per terminare il processo di stampa.
2. Con `lpstat -o` (o con `lpstat -h server-della-stampante -o`) controllate da quale queue si sta stampando e cancellate l'incarico con `cancel` ⟨*queue*⟩-⟨*numero dell'incarico*⟩ (o con `cancel -h print-server` ⟨*queue*⟩-⟨*numero dell'incarico*⟩).
3. Utilizzate eventualmente il comando `fuser`.
4. Resettate la stampante.

Su Ghostscript

Ghostscript accetta dati PostScript e PDF. Per la conversione in altri formati, esso contiene una serie di driver, chiamati “device”

Il processo di conversione di Ghostscript è diviso in due fasi:

1. I dati PostScript vengono trasformati in matrice: la grafica descritta in linguaggio PostScript viene cioè scomposta in un reticolo fine di punti d'immagine. Questa fase è uguale in tutti i driver di Ghostscript. Quanto più fine è il reticolo (ovvero, quanto più alta la risoluzione), tanto migliore sarà la qualità della stampa. Tuttavia, un raddoppiamento della risoluzione orizzontale e verticale necessita un aumento dei punti del reticolo ed una quadruplicazione della memoria necessaria.

2. La grafica scomposta in punti viene ora tradotta dal driver scelto nel formato (linguaggio di stampa) desiderato.

Ghostscript non vi offre solo driver per stampanti. Ghostscript può anche trasformare i file PostScript in file per l'output sullo schermo o in file PDF.

Per trasformare i file PostScript in comodi documenti da visualizzare sullo schermo, usate il programma gv (pacchetto `gv`) che offre un'interfaccia utente grafica per Ghostscript.

Ghostscript è un programma molto versatile e ricco di opzioni per la riga di comando. La documentazione principale su Ghostscript si trova nella pagina di manuale di `gs` (`man gs`). Troverete la lista dei driver di Ghostscript su:

`file:/usr/share/doc/packages/ghostscript/catalog.devices`

e, soprattutto, su:

```
file:/usr/share/doc/packages/ghostscript/doc/index.html
file:/usr/share/doc/packages/ghostscript/doc/Use.htm
file:/usr/share/doc/packages/ghostscript/doc/Devices.htm
file:/usr/share/doc/packages/ghostscript/doc/hpdj/gs-hpdj.
txt
file:/usr/share/doc/packages/ghostscript/doc/hpijs/hpijs_
readme.html
file:/usr/share/doc/packages/ghostscript/doc/stp/README
```

Una chiamata diretta di Ghostscript avvia anche un dialogo con con proprio prompt GS>, da chiudere con il comando `quit`.

Il comando di aiuto `gs -h` elenca tutte le opzioni principali e fornisce una lista attuale dei "device" supportati, indicando solo la denominazione generale del driver, come `uniprint` o `stp` (se un solo driver supporta più modelli). I file con i parametri per `uniprint` ed i modelli di `stp` sono elencati, uno per uno, su `file:/usr/share/doc/packages/ghostscript/catalog.devices`.

Esempi di impiego di Ghostscript

In `file:/usr/share/doc/packages/ghostscript/examples` troverete degli esempi di file PostScript.

L'"ellisse cromatica" `file:/usr/share/doc/packages/ghostscript/examples/colorcir.ps` si adatta bene ad un test di stampa.

Output di X11

Su X, la superficie grafica, potete visualizzare un file PostScript con il comando `gs`:

```
tux@terra:~ >  gs -r60 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps
```

Immettete il comando in una sola riga senza (`'\'`).

Con l'opzione `-r`, viene indicata la risoluzione, che dovrà essere adatta al device in questione (stampante o schermo) (provate con `-r30`). Per chiudere il programma, premete, nella finestra di terminale in cui avete dato il comando `gs`, i tasti Ctrl + C .

Conversione in PCL5e o PCL6

La conversione di un file PostScript in un formato di stampante PCL5e o PCL6 si ha, ad esempio, con il comando:

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=ljet4 -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps
```

laddove il comando dovrà stare in un'unica riga senza (`'\'`). Inoltre, si presuppone che il file `/tmp/out.prn` non esista ancora.

Conversione in PCL3

La conversione di un file PostScript in un formato di stampante PCL3 si ha, ad esempio, con i comandi

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=deskjet -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps
```

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=hpdj -r300x300 \
     -sModel=500 -sColorMode=mono -dCompressionMethod=0 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps

tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=cdjmono -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps

tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=cdj500 -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps

tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=cdj550 -r300x300 \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps
```

(Ogni comando deve entrare in un'unica riga senza `'\'`.)

Conversione in ESC/P, ESC/P2 o matrice ESC/P

La conversione di un file PostScript in un formato di stampante ESC/P2 o ESC/P o ESC/P a matrice si ha, ad esempio, con i comandi:

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     @stcany.upp \
     /usr/share/doc/packages/ghostscript/examples/colorcir.ps \
     quit.ps

tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     -sDEVICE=stcolor -r360x360 \
     -dBitsPerPixel=1 -sDithering=gsmono -dnoWeave \
     -sOutputCode=plain \
```

```
/usr/share/doc/packages/ghostscript/examples/colorcir.ps \
quit.ps
```

È chiara qui la differenza nel richiamo, usando un file di parametri per il driver `uniprint` e con un altro driver di Ghostscript. Dal momento che tutti i parametri del driver si trovano nel file uniprint, non vi è bisogno di indicarne altri, in contrapposizione agli altri driver di Ghostscript.

Stampa diretta

Dopo ogni comando di cui sopra i dati da stampre risiedono in `/tmp/out.prn`, che con il seguente comando di `root` possono ora essere inviati direttamente alla stampante (dunque senza spooler o filtro di stampante), se la stampante è collegata alla prima porta parallela `/dev/lp0`:

```
terra:~ #  cat /tmp/out.prn >/dev/lp0
```

a2ps

Se desiderate stampare un file di testo ASCII con Ghostscript, dovrete prima trasformarla in PostScript, dal momento che Ghostscript si aspetta di ricevere un file PostScript. Per far ciò, usate il programma a2ps (pacchetto `a2ps`).

a2ps è uno strumento potentissimo per la conversione di file ASCII in ottime stampe PostScript.

a2ps è un programma versatile con molte opzioni per la riga di comando. La sua documentazione principale si trova su pagina di manuale di `a2ps` (`man a2ps`) – quella completa nella pagina info di`a2ps`.

Esempi di impiego di a2ps

Stampa diretta di un file di testo con a2ps

Per convertire un file di testo in PostScript con a2ps, in modo che un foglio contenga due pagine ridotte, potete inserire il seguente comando:

```
tux@terra:~ >  a2ps -2 --medium=A4dj --output=/tmp/out.ps file-
     di-testo
```

Potete visualizzare un'anteprima di stampa di a2ps sulla superficie grafica, con il comando

```
tux@terra:~ >  gs -r60 /tmp/out.ps
```

Nella finestra di terminale in cui avete inserito il comando `gs`, dovrete premere invio per passare alla pagina successiva. Per chiudere, premete Ctrl + c.

Per convertire la stampa di a2ps nel formato della stampante, inserite

```
tux@terra:~ >  gs -q -dNOPAUSE -dSAFER -sOutputFile=/tmp/out.prn
     \
     ⟨parametro-del-driver⟩ /tmp/out.ps quit.ps
```

laddove ⟨*parametro-del-driver*⟩ dovrà adattarsi alla stampante. Vd. paragrafo precedente.

Per inviare la stampa di Ghostscript, con diritti `root`, direttamente alla stampante (senza passare per spooler e filtro),

```
terra:~ #  cat /tmp/out.prn >/dev/lp0
```

a condizione che la stampante sia collegata alla prima porta parallela `/dev/lp0`.

Stampare biglietti da visita

Per darvi un assaggio della versatilità di a2ps, stamperemo ora dei semplici biglietti da visita. Create un biglietto da visita come semplice file di testo `card`

```
Titolo Nome Cognome
Via
CAP Località
E-mail: user@domain
Telefono: prefisso-numero
```

file 23: *card: un biglietto da visita*

Aggiungete il simbolo ASCII\f (formfeed), in modo che a2ps stampi ogni biglietto come una pagina a se stante.

```
tux@terra:~ >  echo -en "\f" >>card
```

Riproduzione in 10 pezzi in un file `cards`:

```
tux@terra:~ >  for i in $(seq 1 10) ; do cat card >>cards ; done
```

Determinare la riga più lunga su `cards`:

```
tux@terra:~ >  cat cards | wc -L
```

Covertire in PostScript, in modo tale che tutti i 10 biglietti da visita siano distribuiti in due colonne di 5 biglietti ciascuna per ogni foglio, con una cornice su ogni biglietto e con un testo non eccedente la riga più lunga, senza intestazione o pié di pagina:

```
tux@terra:~ >  a2ps -i -j --medium=a4dj --columns=2 --rows=5 \
     --no-header --chars-per-line=numero --output=cards.ps cards
```

Il comando deve occupare una sola riga senza (`'\'`) e per `numero` impostate il numero di caratteri della riga più lunga.

Controllate allo schermo con `gs -r60 cards.ps` ed avviate la stampa come sopra descritto, oppure con il comando `lpr` e con il sistema di stampa di `lpr cards.ps`.

Convertire in PostScript con psutils

Per convertire, stampate da una applicazione in un file `/tmp/in.ps` e con `file /tmp/in.ps` potete verificare che si tratti effettivamente di un file PostScript.

Programmi, per convertire dati PostScript, si trovano nel pacchetto `psutils`. Soprattutto il programma `pstops` consente tanto per quanto rigurda la conversione. Vedi le di pagina di manuale di `pstops` (`man pstops`). Il pacchetto `psutils` non viene installato di default, dunque dovete installarlo.

I comandi riportati di seguito funzionano solo con file PostScript, creati in modo da consentire una conversione, cosa che di solito è possibile, ma a seconda degli applicativi con cui è stato creato il file PostScript, può rilevarsi impossibile.

psnup

Con

```
tux@terra:~ >  psnup -2 /tmp/in.ps /tmp/out.ps
```

`/tmp/in.ps` diventa `/tmp/out.ps` con due pagine rimpicciolite l'una accanto all'altra su un foglio. Visto che cresce la complessità del processo di stampa, quando si tratta di riprodurre più pagine di dimensioni ridotte su di un solo foglio, alcune stampanti PostScript con poca memoria integrata, possono fallire nel tentativo di stampare incarichi diventati troppo complessi.

pstops

pstops consente di impostare la dimensione e posizione nel modo desiderato:

```
tux@terra:~ >  pstops '1:0@0.8(2cm,3cm)' /tmp/in.ps /tmp/out.ps
```

Con il fattore 0.8 una pagina A4 di ca. 21x30 cm viene scalata (ridotta) a ca. 17x24 cm.; ne risulta un ulteriore margine a destra di ca. 4 cm e nella parte superiore di ca. 6 cm, ed inoltre il tutto viene spostato di 2 cm verso destra e di 3 cm in alto, per avere tutti i margini di uguale dimensione.

Con il comando pstops si riesce a ridimensionare di molto ed inoltre utilizza margini generosi, dunque si adatta particolarmente per quei applicativi che fanno rientrare tanto in una pagina - per cui al momento della stampa ti `/tmp/in.ps` non tutto avrebbe trovato posto su un foglio.

Con

```
tux@terra:~ >  pstops '1:0@0.8(2cm,3cm)' /tmp/in.ps /tmp/out1.ps
tux@terra:~ >  psnup -2 /tmp/out1.ps /tmp/out.ps
```

si hanno due pagine ridimensionate di molto l'una accanto all'altra su un foglio – però con tanto spazio tra le due pagine ridimensionate.

Si raggiungono miglior risultati se si posizionano le singole pagine in modo mirato:

```
tux@terra:~ >  pstops '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)' \
     /tmp/in.ps /tmp/out.ps
```

Il comando va immesso senza '\' su una riga sola.

L'effetto di `pstops '2:0L@0.6(20cm,2cm)+1L@0.6(20cm,15cm)'`:

2:0 ... +1 significa che 2 pagine vengono sovrapposte laddove le pagine modulo 2 contano come pagina 0 (modulo 2) e pagina 1 (modulo 2).

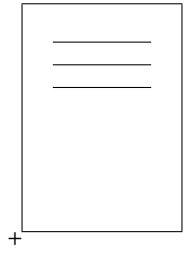
0L@0.6(20cm,2cm) significa, che la pagina 0 (modulo 2) viene girata per 90 gradi verso sinistra, scalata con il fattore 0.6, e in seguito spostata di 20cm verso destra e di 2cm in alto.

1L@0.6(20cm,15cm) In modo anologo la pagina 1 (modulo 2) viene girata di 90 gradi verso sinistra, scalata con il fattore 0.6, ed in seguito spostata di 20cm verso destra e di 15cm in alto.

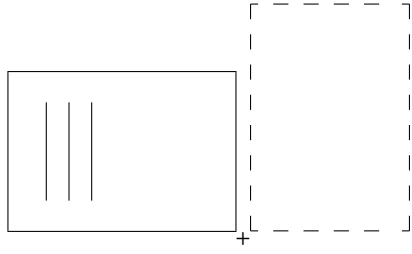
Illustrazione:

In PostScript il punto zero di un sistema di coordinate è l'angolo in basso a sinistra del foglio, che qui viene contrasseganto con +.

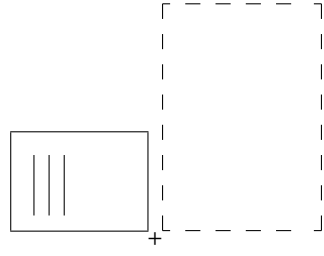
Ecco una pagina 0 (modulo 2) con tre righe di testo:



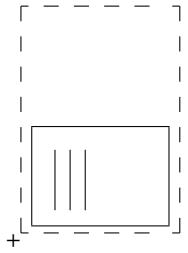
Dopo una rotazione verso sinistra di 90 gradi:



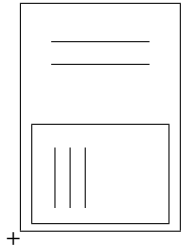
Dopo essere stata scalata con un fattore di 0.6:



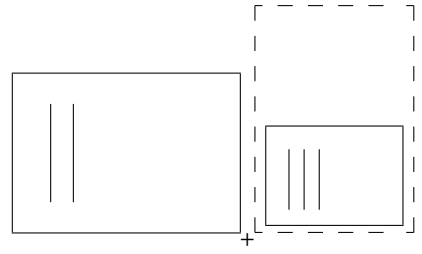
Dopo essere stata spostata di 20cm verso destra e di 2cm verso l'alto:



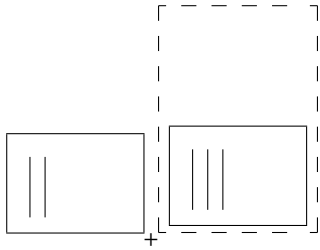
Sovrapposizione della pagina 1 (modulo 2) con due righe di testo:



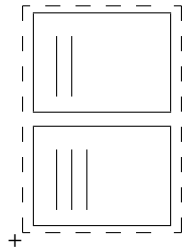
Dopo una rotazione verso sinistra della pagina 1 (modulo 2) di 90 gradi:



Dopo aver scalato la pagina 1 (modulo 2) con il fattore 0.6:



Dopo aver spostanto la pagina 1 (modulo 2) di 20 cm verso destra e 15 cm in alto:



psselect

Con psselect potete selezionare singole pagine.

Con

```
tux@terra:~ >  psselect -p2,3,4,5 /tmp/in.ps /tmp/out.ps
```

oppure

```
tux@terra:~ >  psselect -p2-5 /tmp/in.ps /tmp/out.ps
```

selezionate da /tmp/in.ps le pagine 2,3,4 e 5 e vengono emesse da /tmp/out.ps.

Con

```
tux@terra:~ >  psselect -p1,2,3,4 /tmp/in.ps /tmp/out.ps
```

oppure

```
tux@terra:~ >  psselect -p-4 /tmp/in.ps /tmp/out.ps
```

selezionate le pagine 1,2,3 e 4

```
tux@terra:~ >  psselect -p2,2,2,5,5 /tmp/in.ps /tmp/out.ps
```

selezionate tre volte la pagina 2 e due volte la pagina 5

```
tux@terra:~ >  psselect -p3- /tmp/in.ps /tmp/out.ps
```

selezionate dalla pagina 3 fino all'ultima pagina

```
tux@terra:~ >  psselect -p_1 /tmp/in.ps /tmp/out.ps
```

selezionate solo l'ultima pagina

```
tux@terra:~ >  psselect -p_4-_2 /tmp/in.ps /tmp/out.ps
```

selezionate dalla quart'ultima fino alla penultima pagina.
Con

```
tux@terra:~ >  psselect -r -p3-5 /tmp/in.ps /tmp/out.ps
```

vengono selezionate da /tmp/in.ps le pagine 3,4 e 5 ed emesse in ordine inverso in /tmp/out.ps e con

```
tux@terra:~ >  psselect -r -p- /tmp/in.ps /tmp/out.ps
```

vengono emesse nell'ordine inverso tutte le pagine.

Verifica allo schermo con Ghostscript

Il file PostScript `/tmp/out.ps` si lascia visualizzare con la superficie grafica di Ghostscript con `gs -r60 /tmp/out.ps` pagina per pagina. Premendo il tasto invio nella finestra di terminale nella quale avete richiamato Ghostscript, il file PostScript viene visualizzata pagina per pagina. Per chiudere, premete Ctrl + c.

Il programma `gv` nel pacchetto `gv` è un front-end grafico per Ghostscript. Viene richiamato con la superficie grafica con `gv /tmp/out.ps` e consente soprattutto una adeguata rappresentazione per il formato orizzontale, ingrandimento o ridimensionamento (però non nel file PostScript) e la selezione di singole pagine - soprattutto anche per stampare direttamente da `gv`.

La codificazione di testi ASCII

Ogni carattere di un testo è rappresentato da una combinazione di numeri. Quale codice corrisponda a quale carattere è fissato in una tabella. A seconda di quale tabella usi un determinato programma o il filtro della stampante, la rappresentazione del medesimo codice può produrre sullo schermo un carattere diverso da quello prodotto nella stampa.

Con set di caratteri standard sono possibili solo codici da 0 fino a 255.

I caratteri con i codici 0 fino a 127 sono i caratteri ASCII (in particolare le lettere, cifre e caratteri speciali “soliti”, non inclusi sono i caratteri speciali di un determinato paese/lingua), che sono fissati sempre nel modo identico.

I codici 128 fino a 255 sono riservati per caratteri speciali in ogni lingua (per esempio gli umlaut tedeschi).

Dato che vi sono molto più di 128 caratteri specifici di una lingua, i codici 128 fino a 255 non sono dappertutto uguali, ma a secondo della lacazione geografica lo stesso codice viene utilizzato per i diversi caratteri specifici di una lingua.

ISO-8859-1 (o Latin 1) è il sistema di codificazione per le lingue dell’Europa occidentale, mentre ISO-8859-2 (o Latin 2) è la codificazione delle lingue dell’Europa centro-orientale. Quindi per esempio il codice 241 (ottale) secondo ISO-8859-1 è un punto esclamativo capovolto, mentre secondo ISO-8859-2 un‘A maiuscola con l‘ogonek. ISO-8859-15 e ISO-8859-1 sono quasi del tutto simili, con la differenza, ad esempio, che ISO-8859-15 contiene il simbolo dell’euro (codice 164).

Esempio

Tutti i comandi dovranno entrare in una sola riga, senza (‘\’) a *fine riga*.

Generare un file esempio di testo ASCII con

```
tux@terra:~ >  echo -en "\rCode 241(octal):  \
     \241\r\nCode 244(octal):  \244\r\f" >example
```

Visualizzazione allo schermo

Aprire tre finestre di terminale nell‘interfaccia grafica con

```
tux@terra:~ >  xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-1 \
     -title iso8859-1 &
```

```
tux@terra:~ >  xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-15 \
     -title iso8859-15 &
tux@terra:~ >  xterm -fn -*-*-*-*-*-*-14-*-*-*-*-*-iso8859-2 \
     -title iso8859-2 &
```

In ogni finestra di terminale, visualizzare il file d'esempio con i comandi

```
tux@terra:~ >  cat example
```

Su "iso8859-1" avrete:
Code 241 come punto esclamativo capovolto (spagnolo)
Code 244 come cerchio con uncino (simbolo di valuta)

Su "iso8859-15" avrete:
Code 241 come punto esclamativo capovolto (spagnolo)
Code 244 come simbolo dell'euro

Su "iso8859-2" avrete:
Code 241 come A maiuscola con virgoletta (l'ogonek)
Code 244 come cerchio con uncino (simbolo di valuta)

A causa della codificazione stabilita non è possibile usare contemporaneamente tutti i caratteri speciali di diverse lingue. Così per esempio il simbolo dell'Euro non può essere utilizzato assieme alla A con l'ogonek nello stesso testo.

Per ulteriori approfondimenti sulla codificazione giusta, consultate:

Su "iso8859-1" la pagina di manuale di `iso_8859-1` (`man iso_8859-1`).

Su "iso8859-15" la pagina di manuale di `iso_8859-15` (`man iso_8859-15`).

Su "iso8859-2" la pagina di manuale di `iso_8859-2` (`man iso_8859-2`).

Stampa

A seconda della codificazione impostata per una queue, la stampa di testi ASCII (ovvero del file `example`) avviene come negli esempi. La stampa di documenti approntati con sistemi di videoscrittura non ne viene influenzata, poiché questi sistemi inviano alla stampante dati in formato PostScript e non ASCII.

Stampando `example`, si otterrà la codificazione utilizzato nel sistema di stampa per il testo ASCII.

Con `a2ps` è possibile convertire il file `example` in PostScript, e stabilire il sistema di codificazione:

```
tux@terra:~ >  a2ps -1 -X ISO-8859-1 -o example-ISO-8859-1.ps
     example
```

```
tux@terra:~ >  a2ps -1 -X ISO-8859-15 -o example-ISO-8859-15.ps
     example
tux@terra:~ >  a2ps -1 -X ISO-8859-2 -o example-ISO-8859-2.ps
     example
```

Se si stampano i file PostScript `example-ISO-8859-1.ps`, `example-ISO-8859-15.ps` ed `example-ISO-8859-2.ps`, allora si avrà il sistema di codificazione stabilito con `a2ps`.

Stampare nella rete TCP/IP

Per informazioni utili sullo spooler di stampante LPRng consultate *LPRng-Howto* sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html`

Per CUPS vedi *CUPS Software Administrators Manual* sotto
`file:/usr/share/doc/packages/cups/sam.html`

Denominazione

Server di stampante Di seguito chiameremo “server di stampante” un computer completo con sufficiente potenza di calcolo e capacità di memoria.

Box di server di stampante e stampanti di rete

- Una “box di server di stampante” è un piccolo dispositivo con una connessione di rete TCP/IP da una parte ed la possibilità di connessione locale per una stampante dall’altra. Vi sono anche “box di router” che dispongono di una possibilità di connessione per una stampante e che vanno trattati come box di server di stampante.
- Una “stampante di rete” dispone di una propria connessione di rete TCP/IP. In fin dei conti si tratta di una stampante con box di server di stampante integrata. Stampanti di rete e box di server di stampanti vanno dunque trattati allo stesso modo.

Sussiste una grande differenza tra una stampante di rete o box di server di rete da una parte e un server di stampante vero e proprio dall’altra. Vi sono anche grandi stampanti che forniscono a corredo un computer completo come server della stampante per il processo di stampa in una rete. Ma in questo caso per stampare, viene indirizzato il server della stampante fornito a corredo, e non la stampante.

Stampare protocolli nella rete TCP/IP

Vi sono le seguenti possibilità per stampare in una rete TCP/IP che si distinguono non tanto per quanto riguarda l'hardware impiegato, ma per il protocollo utilizzato. Per tale ragione durante la configurazione della stampante di YaST2 si distingue in base al protocollo e non in base all'hardware.

Stampare tramite il protocollo LPD
L'incarico di stampa viene inviato tramite il protocollo LPD a una queue remota. Chiaramente l'emittente e il destinatario supportano il protocollo LPD.

Emittente

LPRng
LPRng supporta il protocollo LPD tramite lpd. Serve una queue locale tramite la quale l'lpd locale può inoltrare l'incarico di stampa tramite il protocollo LPD ad una queue remota.
Nel caso di LPRng ciò funziona anche senza lpd locale. Il programma `lpr` dal pacchetto `lprng` inoltra l'incarico di stampa tramite il protocollo LPD direttamente alla queue remota.

CUPS
CUPS supporta il protocollo LPD esclusivamente tramite il demone CUPS cupsd. Serve una queue locale tramite la quale il cupsd locale può inoltrare l'incarico di stampa tramite il protocollo LPD alla queue remota.

Destinatario

Server della stampante
La stampante è collegata localmente ad un server di stampa ed il server della stampante è indirizzabile tramite il protocollo LPD.

Stampante di rete o box di stampante di rete
La stampante di rete o box di stampante di rete devono essere indirizzabili tramite il protocollo LPD, cosa che di solito è così.

Stampare tramite protocollo IPP
L'incarico di stampa viene inviato ad una queue remota tramite il protocollo IPP. Sia emittente che destinatario devono supportare il protocollo IPP.

Emittente

LPRng

Attualmente LPRng non supporta il protocollo IPP.

CUPS

CUPS supporta il protocollo IPP tramite il cupsd. Serve una queue locale tramite la quale l'lpd locale inoltra l'incarico di stampa tramite il protocollo IPP alla queue remota.
Nel caso di CUPS questo funziona anche senza cupsd locale. Il programma `lp` dal pacchetto cups-client, xpp o il programma KDE `kprinter` possono inoltrare l'incarico di stampa direttamente alla queue remota tramite il protocollo.

Destinatario

Server della stampante

La stampante è collegata ad un server della stampante locale e il server della stampa è indirizzabile tramite il protocollo IPP.

Stampante di rete o box della stampante di rete

La stampante di rete o box della stampante di rete devono essere indirizzabili tramite il protocollo LPD, cosa che è possibile solo con alcuno dispositivi recenti.

Stampare direttamente tramite socket TCP

In questo caso l'incarico della stampante non viene inviato ad una queue remota, poiché non vi è alcun protocollo (né LPD né IPP), che riesca a gestire incarichi di stampa o queue. Invece i dati specifici per la stampante vengono inviati tramite il socket TCP ad una porta TCP remota che deve essere supportata sia dall' emittente che dal destinatario.

Emittente

LPRng/lpdfilter

LPRng supporta il processo di stampa direttamente servendosi del socket TCP via l'lpd. Serve una queue locale attraverso la quale l'lpd locale possa inviare l'incarico di stampa, con i dati specifici della stampante convertiti grazie all'lpdfilter, alla porta TCP remota attraverso il socket TCP.
Nel caso di LPRng questo si può fare anche senza lpd locale. L'opzione `-Y` del programma `lpr` dal pacchetto `lprng` invia i dati dell'incarico di stampa via socket TCP direttamente alla porta TCP remota. Vedi la di pagina di manuale di `lpr` (`man lpr`). Comunque questo avviene senza filtro di stampante frapposto, così l'incarico di stampa deve già contenere i dati specifici per la stampante.

CUPS

CUPS supporta il processo di stampa direttamente tramite il socket TCP solo attraverso il cupsd. Serve una queue locale tramite la quale il cupsd locale possa convertire l'incarico di stampa in dati specifici per la stampante, e poi inviarli via socket TCP-Socket alla porta remota TCP.

Destinatario

Stampante di rete o box della stampante di rete

La stampante di rete o box della stampante di rete di solito dispongono di una porta TCP attraverso la quale possono essere inviati direttamente alla stampante i dati da stampare, ed essere stampati direttamente .

Nel caso della stampante di rete HP o box della stampante di rete HP JetDirect, si tratta di solito della porta 9100 o nel caso di box della stampante di rete JetDirect, con due o tre connessioni per stampanti locali, le porte 9100, 9101 e 9102. Queste porte vengono usate anche da tante altre box della stampante di rete. Consultate il manuale della box della stampante di rete e chiedete in caso di dubbio alla casa produttrice della box della stampante di rete/ stampante di rete, attraverso quale porta la stampante possa essere indirizzata direttamente.

Informazioni a riguardo nel *LPRng-Howto* sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html`
e lì in particolare sotto
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#SECNETWORK`
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#SOCKETAPI`
`file:/usr/share/doc/packages/lprng/LPRng-HOWTO.html#AEN4858`

Stampare tramite il protocollo SMB

L'incarico di stampa, che deve già contenere dati specifici per la stampante, viene inviato tramite protocollo SMB a "share" remote assegnate ad una stampante remota. L'emittente ed il destinatario devono supportare il protocollo SMB. Né LPRng né CUPS supportano direttamente il protocollo SMB. Il sistema di stampa LPRng/lpdfilter usa però smbclient e CUPS usa smbspool (entrambi da pacchetto `samba-client`). Così entrambi i sistemi di stampa supportano seppure indirettamente il protocollo SMB.

Emittente

LPRng/lpdfilter
LPRng supporta il protocollo SMB tramite l' lpdfilter. E'necessaria una queue locale tramite la quale l'lpd locale possa convertire l'incarico di stampa col lpdfilter in dati specifici per la stampante, e poi l'lpdfilter invia questi dati servendosi del smbclient tramite il protocollo SMB alla share remota.

CUPS
E'necessaria una queue locale tramite la quale il cupsd locale possa convertire l'incarico di stampa in dati specifici per la stampante, e poi questi dati vengono inviati con smbspool tramite il protocollo SMB alla share remota.

Destinatario

Il server della stampante SMB
La stampante è connessa ad un server della stampante SMB. Un server della stampante SMB è normalmente un computer DOS/Windows. Può comunque rivestire questo ruolo anche un server Samba Linux.
Il server della stampante SMB è indirizzabile tramite il protocollo SMB. L'accesso alla stampante (cioè l'accesso alla share corrispondente alla stampante) è attivato in quella sede.

Filtraggio durante il processo di stampa nella rete

Vi sono le diverse possibilità descritte di seguito in tema di filtraggio durante il processo di stampa nella rete. E' a questo punto che il file di partenza deve essere convertito nel formato, che la stampante riesce ad elaborare – ovvero in formato che la stampante "comprende" (PostScript, PCL, ESC/P).

La conversione viene realizzata dal filtro della stampante che può funzionare solo su un computer con sufficiente potenza di calcolo e capacità di memoria. Se per stampanti non-PostScript i dati da stampare vengono generati con Ghostscript, serve tanta potenza di calcolo soprattutto per stampe cromatiche ad alta risoluzione o fotostampe.

Le stampante di rete e box di server della stampante di solito non hanno un filtro della stampante integrato, perciò è necessario un server della stampante.

Quando si impiega una stampante PostScript, si può anche rinunciare ad un server della stampante. Le stampanti PostScript spesso riescono automaticamente a distinguere tra testo ASCII e PostScript, e riescono a stampare entrambi i formati. Per quanto rigurda caratteri speciali di una particolare

lingua in testo ASCII, nella stampante va impostata l'adeguata codificazione di set di caratteri. Il testo ASCII deve prima essere convertito in PostScript tramite `a2ps` con codificazione adatta di set di caratteri, o visto che gli applicativi di solito stampano solo testo ASCII o PostScript, in questi casi, se si stampa solo saltuariamente, non è strettamente necessario disporre di un server della stampante.

Le stampanti di rete e le box di server della stampante spesso, se c'è molto da stampare, risultano sovraccariche, in questi caso è necessario un server della stampante con sufficiente capacità di memoria per consentire che gli incarichi vengono memorizzati temporaneamente.

Premesse

La stampante deve venire supportata da SuSE Linux Enterprise Server, dato che il filtro genera i dati specifici per la stampante come per una stampante collegata localmente; vd. a riguardo la sezione *Configurazione manuale di porte di stampanti locali* a pagina 70 ss.

Denominazione

- Il "client" è il computer sul quale viene generato l'incarico di stampa.
- "Box di server della stampante" indica sia la stampante di rete che la box di server della stampante, visto che possono essere trattati alla stessa maniera.
- Con "server della stampante" qui è inteso un solo computer centrale cui tutti i client inviano i loro incarichi. Il server della stampante inoltra i dati alle sue stampanti collegate in locale o tramite rete TCP/IP alle box di server della stampante.
- "Forward" indica una queue che non filtra gli incarichi di stampa, ma che inoltra solo a queue remote.
- "Filtro" indica in generale una queue che filtra incarichi di stampa.
- "Prefiltro" indica una queue che filtra incarichi di stampa e che inoltra il risultato ad una queue Forward sullo stesso computer.
- "Filtro+Forward" indica una queue filtrante incarichi di stampa che inoltra il risultato ad una queue remota.
- "Filtro+Porta" indica una queue filtrante incarichi di stampa che inoltra il risultato ad una porta TCP remota.
- Eventualmente a queste denominazione viene anteposto "LPD", "IPP" e "SMB" per indicare il protocollo usato.

Possibilità di filtraggio nel processo di stampa nella rete

Box di server della stampante con filtraggio sul client

Dato che il processo del filtraggio avviene sul client, esso deve avere un sistema di stampa completo funzionante – dunque o il sistema di stampa LPRng/lpdfilter o il completo sistema di stampa CUPS.

Client utilizza il protocollo LPD (LPRng CUPS)

Prima Prefiltro e dopo Forward (solo LPRng)

Il metodo classico consiste di due queue sul client: una queue per il filtraggio e una per l'inoltro.

1. Client: convertire l'incarico di stampa in dati da stampare (Prefiltro) e trasmettere alla queue Forward come nuovo incarico di stampa.
2. Client: la queue Forward inoltra i dati da stampare alla box del server della stampante (LPD-Forward)
3. Box del server della stampante LPD: inviare alla stampante i dati da stampare

Filtro+Forward (LPRng e CUPS) Qui si avviene il filtraggio e l'inoltro ad una queue. Con LPRng questo viene indicato con "lpr-bounce" o "lpd-bounce".

1. Client: convertire l'incarico in dati da stampare e inoltrare alla box del server della stampante (Filtro+ Forward LPD)
2. Box del server della stampante LPD: inviare i dati da stampare alla stampante

Client utilizza il protocollo IPP (solo CUPS)

Filtro+Forward (solo CUPS)

1. Client: convertire l'incarico in dati da stampare ed inviare alla box del server della stampante (Filtro+Forward IPP)
2. Box del server della stampante IPP: inviare i dati da stampare alla stampante

Client usa socket TCP (LPRng e CUPS)

Filtro+Porta (LPRng e CUPS)

1. Client: convertire l'incarico in dati da stampare e inviare alla box del server della stampante (Filtro+Porta)
2. Box del server della stampante: inviare dati da stampare alla stampante.

Box del server della stampante con filtraggio sul server della stampante

Dato che il filtraggio avviene sul server della stampante deve girarci un sistema di stampa completo con demone – dunque alla maniera del sistema di stampa LPRng/lpdfilter o il sistema di stampa CUPS.

Dato che il filtraggio avviene sul server della stampante, sul client non deve trovarsi un sistema di stampa completo, se sul client gli incarichi di stampa possono essere inviati direttamente al server della stampante tramite il comando `lpr` (per LPRng) o del comando `lp` o `xpp` o `kprinter` (per CUPS). In questo caso è la premessa che il server della stampante supporti il protocollo utilizzato dal client (LPD o IPP).

Dopo che il server della stampante riceve un incarico da stampare, lo elabora come descritto nella sezione *Box del server della stampante con filtraggio sul client* per il client.

Il client può inviare al server della stampante l'incarico da stampare tramite un altro protocollo, da quello usato dal server della stampante per inviare i dati da stampare alla box del server della stampante.

Client usa il protocollo LPD (solo LPRng)

Direttamente (solo LPRng)

1. Client: inviare incarico da stampare a server della stampante (comando `lpr`)
2. server della stampante LPD: convertire l'incarico da stampare in dati da stampare, e inviare dati della stampante alla box del server della stampante.

Forward (solo LPRng)

1. Client: inviare incarico da stampare al server della stampante (Forward LPD)
2. Server della stampante LPD: convertire l'incarico da stampare in dati della stampante e inviarli alla box del server della stampante.

Client usa il protocollo IPP (solo CUPS)

Direttamente (solo CUPS)

1. Client: inviare l'incarico da stampare al server della stampante (comando `lp` o `xpp` o `kprinter`)
2. Server della stampante IPP: convertire l'incarico da stampare in dati da stampante e inviarli alla box del server della stampante.

Stampante annessa al print server con filtraggio sul print server
Se la stampante è collegata direttamente al server della stampante, si ha la stessa situazione descritta in *Box del server della stampante con filtraggio sul server della stampante* (vd. 127), con la sola differenza che, invece di "inviare i dati della stampante alla box del server della stampante" deve esserci "inviare i dati della stampante alla stampante".

Stampante collegata ad un server di stampante con filtraggio sul client
Per il server della stampante LPD ed IPP di solito ciò non conviene. Su ogni client dovrebbe esserci un completo sistema di stampa configurato e funzionante, mentre dovrebbe bastare una configurazione come descritta nella sezione *Stampante collegata ad un server di stampante con filtraggio sul server della stampante*.

Server di stampante SMB con filtraggio sul client
Sul server di stampante SMB non è previsto alcun filtraggio. Sotto questo aspetto il server di stampante SMB è simile alla box del server della stampante.

Client usa il protocollo SMB (LPRng e CUPS)

Filter+SMB-Forward (LPRng u CUPS)

1. Client: convertire incarico di stampa in dati per la stampante e inviare al server della stampante SMB (Filter+SMB-Forward)
2. Server della stampante SMB: inviare dati per la stampante alla stampante.

Risolvere dei problemi

Rete TCP/IP
La rete TCP/IP e la risoluzione dei nomi devono funzionare (vedi *Fondamenti del collegamento in rete* a pagina 203).

Controllare la configurazione del filtro
Collegate la stampante direttamente alla prima porta parallela del computer. Configurate la stampante solo ai fini del test come stampante locale per escludere dei problemi dovuti alla rete. Se la stampante funziona in locale, state usando i giusti driver Ghostscript e parametri per la configurazione del filtro.

Testare un lpd remoto
Con

```
terra:~ #  netcat -z host 515 && echo ok || echo failed
```

potete verificare se è possibile un collegamento TCP al lpd (Port 515) sul computer `host`. In caso negativo, il problema è dovuto o all' lpd o alla rete.

Come utente `root` con

```
terra:~ #  echo -e "\004queue" | netcat -w 2 -p 722 host 515
```

si ottiene un resoconto (a volte molto dettagliato) sulle `queue` che si trovano sull' `host` remoto, sempre che l'lpd del computer remoto funzioni ed è possibile inviarci delle richieste. Se l'lpd non risponde, ci sono due possibilità: o non funziona l'lpd, o vi è una grave disfunzione della rete. Se ottenete una risposta dall'lpd, questa dovrebbe chiarire, la ragione per cui sulla `queue` di `host` non sia possibile stampare – esempi:

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

output 2: *Messaggio di errore di lpd*

Nel caso di una risposta simile dell'lpd, il problema è dovuto all'lpd remoto.

Testare il cupsd remoto

Con

```
terra:~ #  netcat -z host 631 && echo ok || echo failed
```

si può verificare se è possibile un collegamento TCP al cupsd (Port 631) sull'`host`. In caso negativo, il problema è dovuto o alcupsd o alla rete.

Con

```
terra:~ #  lpstat -h host -l -t
```

si ottiene un resoconto (a volte molto dettagliato) sulle `queue` che si trovano sull' `host` remoto, sempre che il cupsd del computer remoto funzioni ed è possibile inviarci delle richieste.

Con

```
terra:~ #  echo -en "\r" | lp -d queue -h host
```

si può verificare se le queue sull' host accettino un incarico di stampa, laddove l'incarico consiste di un solo carattere di ritorno di carrello – cioè si vuole eseguire solo un test senza stampare effettivamente – e se si vuole stampare, allora solo un foglio bianco.

Testare un server SMB remoto

La funzione principale si lascia testare con:

```
terra:~ #  echo -en "\r" | smbclient '//HOST/SHARE'
    'PASSWORD' \
    -c 'print -' -N -U 'USER' && echo ok || echo failed
```

su una sola riga senza backlash, '\'. Al posto di HOST inserite il nome del computer del server Samba, per SHARE il nome della queue remota (cioè i nome della share Samba), per PASSWORD la vostra password e per USER il nome dell'utente. Con questo comando si esegue solo un test, normalmente non dovrebbe venir stampato alcunché – e se sì, allora solo un foglio bianco.

Con

```
terra:~ #  smbclient -N -L host
```

visualizzate le share disponibili suhost – vd. la pagina di manuale di smbclient (man smbclient).

La stampante di rete o la box del print server non funzionano ineccepibilmente

Di solito si verificano dei problemi con lo spooler della stampante che gira in una box del server della stampante, non appena c'è tanto da stampare. Visto che il problema è dovuto alla box del server della stampante, non può essere risolto.

Si può aggirare lo spooler indirizzando direttamente la stampante collegata alla box del server della stampante tramite il socket TCP.

In questo modo la box del server della stampante converte solamente tra le diverse forme di trasmissione dei dati (rete TCP/IP e collegamento della stampante locale), così la stampante collegata alla box del server della stampante si comporta come una stampante collegata in locale. Avrete un controllo più diretto sulla stampante, più di quanto con lo spooler sulla box del server della stampante frapposto.

Deve essere noto la relativa porta TCP sulla box del server della stampante.

Se la stampante è collegata alla box del server della stampante ed è accesa, la porta TCP in questione si lascia determinare in poco tempo dopo aver acceso la box del server della stampante con il programma `nmap` dal pacchetto `nmap`.

`nmap` emettera nel caso di una box del server della stampante:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

- Tramite `telnet` potete entrare nella box del server della stampante. Lì potete richiedere informazioni basilari e configurare.
- Tramite HTTP potete indirizzare un server web che gira su una box del server della stampante. Esso fornisce informazioni dettagliate e permette di configurare in modo dettagliato.
- Attraverso la porta 515 potete indirizzare lo spooler che gira sulla box del server della stampante tramite il protocollo LPD.
- Attraverso la porta 631 potete indirizzare lo spooler che gira sulla box del server della stampante tramite il protocollo IPP.
- Attraverso la porta 9100 potete indirizzare la stampante collegata alla box del server della stampante tramite socket il TCP.

Server della stampante LPD ed IPP

Solo con CUPS

Un server CUPS supporta solitamente solo il protocollo IPP. Il programma `/usr/lib/cups/daemon/cups-lpd` dal pacchetto cups permette comunque, che un server CUPS accetti anche incarichi di stampa inviatigli alla porta 515 tramite il protocollo LPD. Dovete abilitare il relativo servizio per l'`inetd` con YaST2 o manualmente, attivando la riga corrispondente nel file `/etc/inetd.conf`.

LPRng/lpdfilter e CUPS

Alcuni vorranno far girare entrambi i sistema di stampa LPRng/lpdfilter e CUPS sullo stesso computer – forse per aggiungere CUPS al server della stampante LPD, o perché in alcuni casi particolari necessitano il sistema di stampa LPRng/lpdfilter.

In linea di massima sorgono delle difficoltà se i due sistemi debbano coesistere su un computer. Qui verranno accennati brevemente alcuni dei problemi e le restrizioni che ne risultano. La tematica comunque è troppo complessa per poter descrivere in questa sede una soluzione.

Esistono diverse possibilità. Saremo lieti di fornirvi assistenza nel quadro del nostro servizio SuSE, per i particolari visitate
`http://www.suse.de/en/services/index.html`
.

- La configurazione della stampante non dovrebbe essere eseguita con YaST2, poiché la configurazione della stampante di YaST2 non è adatta per questi casi.
- Vi è un conflitto tra i pacchetti lprng e cups-client, dato che contengono file omonimi per esempio `/usr/bin/lpr` e `/usr/bin/lp`. Quindi non va installato il pacchetto cups-client che a sua volta conduce alla mancanza di tool di riga di comando per CUPS (ve ne sono solo per LPRng). Comunque è possibile stampare servendosi delle queue CUPS attraverso l'interfaccia grafica con xpp o kprinter, e lo è anche da tutti gli applicativi che supportano direttamente CUPS.
- Per motivi di compatibilità, all'avvio cupsd crea un nuovo file `/etc/printcap` con solo i nomi delle queue CUPS, poichè numerosi applicativi leggono i nomi delle queue da `/etc/printcap` per poterli mettere a disposizione nel menu della stampante. Questo non deve avvenire per cupsd, in modo che `/etc/printcap` serva solo per l'uso del sistema di stampante LPRng/lpdfilter. La conseguenza è che gli applicativi che utilizzano solo queue da `/etc/printcap`, mostrano solo le queue locali, e non tutte le queue CUPS disponibili nella rete.

Parte II

System

Il Kernel

Il kernel che durante l'installazione viene scritto sull'hard disk viene configurato in modo da supportare una gamma quanto vasta possibile di componenti hardware e feature del kernel.

Le sorgenti del kernel

Per poter compilare i sorgenti del kernel devono essere stati installati i seguenti pacchetti: i sorgenti del kernel (pacchetto `kernel-source`), il compilatore C (pacchetto `gcc`), i binutils GNU (pacchetto `binutils`) ed i file include per il compilatore C (pacchetto `glibc-devel`). Consigliamo vivamente di installare in ogni caso il compilatore C, poiché il linguaggio C è inseparabilmente legato ai sistemi operativi UNIX. Per poter compilare un kernel a 64 bit su iSeries e pSeries, dovete installare anche pacchetto `cross-ppc64-gcc` e pacchetto `cross-ppc64-gcc`. Questi pacchetti vi permetteranno di eseguire il cosiddetto crosscompiling (compilazione incrociata).

Al kernel iSeries (e anche in minor misura al kernel pSeries) servono alcuni opzioni di configurazione specifiche per un funzionamento senza intoppi. La via più semplice è quella di utilizzare come la base per un nuovo kernel config. un file di configurazione di cui sapete che funziona. La configurazione di default viene memorizzata in `/boot/vmlinuz-<version>.config`. Per permettere l'uso di un crosscompiler, dovete aggiungere sempre `sh make_ppc64.sh` come prefisso al comando.

Moduli del kernel

Tanti driver e feature non sono stati più integrati direttamente nel kernel, ma possono essere caricati sotto forma di moduli di kernel mentre il sistema è in esecuzione. La configurazione del kernel determina quali driver vanno integrati direttamente nel kernel e quali caricare come moduli mentre il sistema è in esecuzione.

I moduli del kernel si trovano sotto `/lib/modules/<version>`, laddove <version> è la versione del kernel attuale.

Utilizzo dei moduli

Per l'utilizzo dei moduli si hanno a disposizione i seguenti comandi:

- `insmod`
  insmod carica il modulo richiesto dopo averlo cercato in una sottodirectory di `/lib/modules/<version>`. Comunque, `modprobe` (vedi sotto) dovrebbe essere usato al posto di `insmod` che ha perso in termini di importanza.

- `rmmod`
  Scarica il modulo indicato che è possibile solo se il modulo in questione non è più necessario. Per esempio, non sarà possibile scaricare il modulo isofs (il filesystem del CD-ROM) fintanto che un CD è montato.

- `depmod`
  Questo comando crea un file di nome `modules.dep` nella directory `/lib/modules/<version>`, dove sono definite tutte le dipendenze di tutti i moduli. Ciò è necessario per assicurare che tutti i moduli dipendenti vengano caricati assieme a quelli selezionati. Se START_KERNELD è impostata in `/etc/rc.config`, questo file verrà generato ad ogni avvio del sistema.

- `modprobe`
  Questo comando è molto utile e può venire impiegato anche per altri scopi (p.e. test di tutti i moduli di un determinato tipo finché se ne trovi uno caricabile). Al contrario del caricamento con insmod, modprobe analizza il file `/etc/conf.modules` e dovrebbe perciò venire usato per il caricamento dei moduli. Per una spiegazione dettagliata di tutte le opzioni, leggete le corrispondenti pagine di manuale (ingl.man-page)

- `lsmod`
  Indica quali moduli sono caricati al momento e da quanti altri moduli vengono usati. Moduli caricati dal demone del kernel sono caratterizzati da un tag `autoclean` che indica che questi moduli saranno rimossi automaticamente se per un determinato lasso di tempo non sono stati utilizzati (ingl. idle time limit).

/etc/modules.conf

Il caricamento dei moduli viene inoltre influenzato dal file `/etc/modules.conf`; cfr. la pagina di manuale di `depmod` (`man depmod`).

I parametri per moduli che accedono direttamente all'hardware e perciò necessitano di opzioni specifiche del sistema (per esempio lettori di CD-ROM o driver di rete) possono essere immessi in questo file. I parametri qui registrati sono, in linea di principio, identici a quelli che vengono consegnati al prompt di boot del kernel, in molti casi, comunque, i nomi differiscono da quelli che vengono impiegati al prompt di boot. Se il tentativo di caricare un modulo dovesse fallire, provate a specificare l'hardware in questo file e usate modprobe al posto di insmod per caricare il modulo.

`Modules.conf` dà i nomi di dispositivo per i moduli. Dovreste prima consultare questo file se pensate per esempio che i vostri nomi di dispositivo di rete e driver vengono scambiati.

Particolarità del sistema

Questo capitolo contiene alcune informazioni sul *Filesystem Hierarchy Standard* (FHS) ed il *Linux Standard Base* (LSB), nonché su singoli pacchetti di software e particolarità del caricamento con “initrd”.

Gli standard Linux 142
Esempi di ambienti per FTP ed HTTP 142
Informazioni su pacchetti speciali di software 143
Console virtuali 148
Mappatura della tastiera 148
Adattamenti locali – I18N/L10N 149

Gli standard Linux

Filesystem Hierarchy Standard (FHS)

SuSE Linux Enterprise Server cerca di conformarsi al *Filesystem Hierarchy Standard* (FHS, pacchetto `fhs`); cfr. `http://www.pathname.com/fhs/`. Per questo motivo, di tanto in tanto, è necessario spostare file o indirizzari nei settori "giusti" del filesystem.

Linux Standard Base (LSB)

SuSE supporta il progetto *Linux Standard Base*; per informazioni attuali, vd. `http://www.linuxbase.org`.

Il sistema attuale supporta la specificazione LSB nella versione 1.2; il Filesystem Hierarchy Standard (FHS) è ormai parte integrante della specificazione, che determina anche il formato dei pacchetti e l'inizializzazione del sistema; cfr. capitolo *Il concetto di "boot"* a pagina 159. La specificazione LSB interessa finora solo l'architettura x86

teTeX – TeX su SuSE Linux

TEX è un programma per scrivere testi che gira su numerose piattaforme. E' estendibile tramite macro-pacchetti come LATEX. E' composto da numerosi file, impostate secondo la *TEX Directory Structure* (TDS) (cfr. `ftp://ftp.dante.de/tex-archive/tds/`) teTeX è una raccolta di software TEX aggiornato.

Su SuSE Linux Enterprise Server, teTeX viene usato nella configurazione che debba soddisfare i requisiti della TDS e dell' FHS.

Esempi di ambienti per FTP ed HTTP

Su FTP

Per facilitare l'allestimento di un server FTP, pacchetto `ftpdir` offre un esempio di ambiente, da installare su `/srv/ftp`.

Su HTTP

Apache è il server web standard di SuSE Linux Enterprise Server; assieme all'installazione, vi vengono messi a disposizione dei documenti-esempio sotto `/srv/www/`. Se volete creare un server web proprio, registrate un proprio DocumentRoot in `/etc/httpd/httpd.conf` e archiviate lì i vostri file (documenti, immagini etc.).

Informazioni su pacchetti speciali di software

Il pacchetto bash ed /etc/profile

Quando richiamate una shell di login i file di inizializzazione vengono analizzati da bash in questa sequenza:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Gli utenti non possono eseguire alcune registrazioni in `~/.profile` o `~/.bashrc`. Per garantire un'elaborazione corretta dei file è necessario che le impostazioni basilari di `/etc/skel/.profile` o `/etc/skel/.bashrc` vengono assunte dalla directory dell'utente. Dopo un update si consiglia di orientarsi alle impostazioni di `/etc/skel`; per non perdere propri adattamenti eseguite questi comandi:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

In seguito dovete riscrivere i vostri adattamenti dal file `*.old`.

Il pacchetto cron

Le tabelle cron si trovano su `/var/cron/tabs`. Come tabella valida per tutto il sistema, viene creato il file `/etc/crontab`. Nel file `/etc/crontab`, dopo l'inserimento dell'ora, indicate anche sotto quale utente debba venire eseguito il relativo incarico (cfr. file 24, che indica `root`); i dati dei pacchetti su `/etc/cron.d` hanno lo stesso formato – cfr. la pagina di manuale di `cron` (`man 8 cron`).

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

file 24: *Esempio di valori di /etc/crontab*

`/etc/crontab` *non* può essere modificato con `crontab -e`, ma deve venire direttamente caricato in un editor, modificato, e infine memorizzato.

Alcuni pacchetti installano, nelle directory `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly` degli shell script, la cui elaborazione viene diretta da `/usr/lib/cron/run-crons`. `/usr/lib/cron/run-crons` viene richiamato ogni 15 minuti dalla tabella principale (`/etc/contrab`); in questo modo, si assicura che vengano recuperate per tempo esecuzioni mancate. Non meravigliatevi, quindi, se, subito dopo il boot, appare l'utente `nobody` nella tabella del processo; `nobody` sta probabilmente aggiornando la banca dati locate (vd. sezione *Impostazioni nei file di /etc/sysconfig* a pagina 184).

Gli interventi di manutenzione quotidiani sul sistema sono stati distribuiti su diversi script per motivi di chiarezza (Il pacchetto `aaa_base`). In `/etc/cron.daily` oltre a `aaa_base` vi è per esempio `backup-rpmdb`, `clean-tmp` o `clean-vi`.

File di log – il pacchetto logrotate

Molti servizi di sistema ("daemon") ed il kernel stesso protocollano regolarmente lo stato del sistema od eventi particolari nei cosiddetti log file o file di protocollo, che l'amministratore può consultare in qualsiasi momento per determinare lo stato del sistema in un momento particolare, nonché ricercare ed ovviare ad errori o malfunzionamenti. Come previsto dall'FHS, questi log file vengono normalmente memorizzati nella directory `/var/log`, il cui contenuto aumenta di giorno in giorno. Con l'aiuto del pacchetto `logrotate`, potete tenere sotto controllo il volume dei file di protocollo.

Configurazione

Nel file di configurazione `/etc/logrotate.conf`, viene determinato il comportamento generale. Con include, in particolare, si imposta quali altri file debbano essere valutati; su SuSE Linux Enterprise Server è previsto che i singoli pacchetti di `/etc/logrotate.d` installino dei file (ad esempio, `syslog` o `yast`).

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

file 25: *Esempio di /etc/logrotate.conf*

logrotate, invece, viene controllato tramite cron ed avviato da `/etc/cron.daily/logrotate` una volta al giorno.

Nota

L'opzione create carica in memoria le impostazioni che avreste potuto eseguire come amministratore nei file `/etc/permissions*`. Assicuratevi sempre che le vostre modifiche non creino dei conflitti.

Nota

Pagine di manuale

Per alcuni programmi GNU (per esempio tar), le manual page non vengono più aggiornate. Al loro posto, troverete un sommario nell'edizione `--help` e un manuale dettagliato nei file Info. Info (`info`) è il sistema ipertestuale di GNU. Con `info info` otterrete delle prime istruzioni per l'uso. `info` è accessibile con Emacs `emacs -f info` o semplicemente con il comando `info`

Il comando ulimit

Con il comando `ulimit` (ingl. *user limits*), potrete limitare l'accesso all'uso delle risorse del sistema o visualizzare le risorse. `ulimit` è particolarmente adatto a ridurre la memoria disponibile alle applicazioni. In questo modo, si può impedire che un'applicazione occupi troppo (o tutto lo) spazio di memoria, causando così il blocco del sistema.

Potrete lanciare di `ulimit` in modi diversi. Per limitare l'uso di memoria, usate le opzioni riportate nella tabella 6.1.

`-m`	grandezza massima della memoria fisica
`-v`	grandezza massima della memoria virtuale (swap)
`-s`	grandezza massima dello stack
`-c`	grandezza massima dei core file
`-a`	visualizzazione dei limiti impostati.

Tabella 6.1: `ulimit`*: impostare le risorse dell'utente*

Le impostazioni per l'intero sistema possono venire effettuate in `/etc/profile`. Una delle impostazioni consiste, ad esempio, nell'autorizzare la creazione di quei core file necessari ai programmatori per il "debug". L'utente non è in grado di aumentare i valori impostati dall'Amministratore del sistema in `/etc/profile`; è però possibile inserire determinate impostazioni nel proprio `~/.bashrc`.

```
# Limite della memoria reale:
ulimit -m 98304

# Limite della memoria virtuale:
ulimit -v 98304
```

file 26: *Impostazioni ulimit su ~/.bashrc*

La memoria viene espressa in KB.

Per informazioni più dettagliate, consultate la pagina di manuale di `bash` (`man bash`).

Nota

Non tutte le shell supportano le indicazioni `ulimit`. Se non potete fare a meno di questo tipo di restrizioni, PAM (per esempio `pam_limits`) offre ampie possibilità di impostazione.

Nota

Il comando free

Il nome del comando `free` è un pò fuorviante, dal momento che questo comando serve a verificare quanta memoria venga attualmente usata…

Troverete le informazioni essenziali su `/proc/meminfo`. Al giorno d'oggi, l'utente di un sistema moderno come Linux non dovrebbe preoccuparsene più di tanto. Il concetto di "RAM disponibile" risale a quando non vi erano ancora sistema di gestione unitari della memoria (ingl. *unified memory management*). Il motto di Linux è: *la memoria libera è cattiva memoria* (ingl. *free memory is bad memory*), il che vuol dire che Linux cerca sempre di bilanciare le varie cache, ma di non lasciare mai della memoria del tutto inutilizzata (o libera)

Di per sé, il kernel non sa nulla di programmi o dati dell'utente, perché lui li amministra in cosiddette "Page Cache". Quando la memoria non basta più, parte di questi dati vengono spostati nella partizione swap o nei file dai quali sono stati originariamente estratti con la chiamata di sistema `mmap` (cfr. pagina di manuale di `mmap` (`man 2 mmap`)).

Inoltre, il kernel dispone anche di altre memorie temporanee, come la cosiddetta "slab cache", che contiente anche un buffer usato per le connessioni alla rete. Così si spiegano tutte le differenze tra i denominatori di `/proc/meminfo`. La maggior parte delle cache (ma non tutte) possono essere consultate attraverso `/proc/slabinfo`.

Il file /etc/resolv.conf

La risoluzione del nome viene gestita tramite il file `/etc/resolv.conf`; cfr. sezione *DNS – Domain Name Service* a pagina 230.

Il file `/etc/resolv.conf` viene continuamente attualizzato solo dallo script `/sbin/modify_resolvconf`. A nessun programma è permesso modificare `/etc/resolv.conf` direttamente. Solo così si può assicurare che la configurazione della rete ed i relativi dati rimangono consistenti.

Console virtuali

Linux è un sistema multitasking e multiutente e, anche se avete un sistema per così dire monoutente, imparerete certamente ad apprezzare i vantaggi di queste capacità.

In modo di testo sono a disposizione 6 console virtuali; premendo la combinazione di tasti (Alt) +(F1) fino a (Alt) +(F6), potete passare da una console all'altra. La settima console è riservata a X11. Modificando il file `/etc/inittab`, potete anche determinare il numero di console disponibili.

Se, da X11, volete ritornare su una console di testo senza però chiudere X11, usate la combinazione (Ctrl) +(Alt) +(F1) fino a (Ctrl) +(Alt) +(F6). Con (Alt) +(F7) ritornate a X11.

Mappatura della tastiera

Per uniformare l'impostazione della tastiera nei programmi sono state eseguite delle modifiche ai seguenti file:

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/⟨VERSION⟩/site-lisp/term/*.el
/usr/lib/joerc
```

Queste modifiche si applicano solo alle applicazioni che leggono `terminfo`, o i cui file di configurazione sono stati direttamente modificati (`vi`, `less` etc.). Altre applicazioni non-SuSE devono venire adattate a queste impostazioni di default. Sotto X il tasto compose ("Multi_key") si ottiene tramite la combinazione (Ctrl) + (⇑) (destro); cfr. la registrazione in `/usr/X11R6/lib/X11/Xmodmap`.

Adattamenti locali – I18N/L10N

SuSE Linux Enterprise Server è un prodotto internazionale e può venire adattato alle condizioni locali. Cioè: l'internazionalizzazione ("I18N") consente localizzazioni speciali ("L10N"). Le abbreviazioni I18N e L10N stanno per *internazionalizzazione* e *localizzazione*: rispettivamente la prima e l'ultima lettera, e in mezzo il numero delle lettere omesse.

Le impostazioni vengono eseguite tramite le variabili LC_* definite nel file `/etc/sysconfig/language`. Naturalmente non si tratta solo dell'impostazione della lingua per la superficie e le comunicazioni dei programmi (ingl. *native language support*), ma anche delle categorie per le *notizie* (linguaggio), *classi dei caratteri*, *sequenza della classificazione*, *data e ora*, *numeri* e *valuta*. Ognuna di queste categorie può venire stabilita direttamente tramite una propria variabile o indirettamente tramite una variabile superiore nel file `language` (vedi la pagina di manuale di `locale` (`man 5 locale`)):

1. RC_LC_MESSAGES, RC_LC_CTYPE, RC_LC_COLLATE, RC_LC_TIME, RC_LC_NUMERIC, RC_LC_MONETARY: queste variabili vengono consegnate alla shell senza il prefisso RC_ e determinano le suddette categorie; i file in questione sono elencati qui di seguito.

   L'impostazione attuale può venire richiesta con il comando `locale`.

2. RC_LC_ALL: questa variabile soprascrive, se configurata, i valori della variabile nominata nel punto 1.

3. RC_LANG: questo è il cosiddetto "fallback", nel caso che nessuna delle suddette variabili sia stata configurata; come standard, SuSE Linux Enterprise Server imposta RC_LANG; in questo modo, l'utente può immettere più facilmente propri valori.

4. ROOT_USES_LANG: è una variabile `yes/no`. Se è impostata su `no`, `root` lavora sempre nell'ambiente POSIX..

Le variabili vengono impostate tramite l'editor `sysconfig`.

Il valore di tali variabili è composto dall'indicazione della lingua (ingl. *language code*), paese o territorio (ingl. *country code*), set dei caratteri (ingl. *encoding*) ed opzione (ingl. *modifier*). Le singole indicazioni vengono collegate ai caratteri speciali:

`LANG=`⟨*language*⟩`[[_`⟨*COUNTRY*⟩`].Encoding[@Modifier]]`

Esempi

Impostate sempre la lingua e la nazione insieme. L'indicazione della lingua segue lo standard ISO 639 (http://www.evertype.com/standards/iso639/iso639-en.html e http://www.loc.gov/standards/iso639-2/) I codici dei paesi sono definiti in ISO 3166 (http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html). Logicamente, possono venire scelti solo i valori per il file di descrizione utilizzabili che si trovano sotto /usr/lib/locale. Altri file di descrizione possono venire creati con l'aiuto di localedef preso dai file in /usr/share/i18n. Un file di descrizione per it_IT@euro.UTF-8 viene creato con:

```
terra:~ #  localedef -i it_IT@euro -f UTF-8 it_IT@euro.UTF-8
```

LANG=it_IT.ISO-8859-1

Per la lingua italiana vale il set di caratteri ISO-8859-1 che inoltre contiene anche il simboli dell'Euro; questo set di caratteri si usa se un programma non è stato ancora adattato ad ISO-8859-15.

L'indicazione del set di caratteri (qui ISO-8859-1) viene riconosciuta per esempio da Emacs.

LANG=it_IT@euro

Segue un esempio per settare una opzione (euro). Per impostare it_DE@euro il default per la installazione standard è italiano.

LANG=it_IT.UTF-8

Se lavorate in un xterm Unicode, dovete indicare UTF-8. Se volete lanciare un xterm per UTF-8, si dovrebbe creare un semplice shell-script con il nome uxterm (per esempio); cfr. file 27.

```
#!/bin/bash
export LANG=de_DE.UTF-8
xterm -fn \
 -Misc-Fixed-Medium-R-Normal--18-120-100-100-C-90-ISO10646-1 \
 -T 'xterm UTF-8' $*
```

file 27: *uxterm per avviare un xterm Unicode*

SuSEconfig elenca le variabili /etc/sysconfig/language e scrive le indicazioni su /etc/SuSEconfig/profile e /etc/SuSEconfig/csh.cshrc. /etc/SuSEconfig/profile viene letto da /etc/profile e

/etc/SuSEconfig/csh.cshrc da /etc/csh.cshrc. In questo modo le impostazioni sono disponibili per tutto il sistema.

Gli utenti possono soprascrivere le predisposizioni del sistema in ~/.bashrc. Se la predisposizione è de_DE e l'utente non è soddisfatto delle comunicazioni del programma in lingua tedesca, può cambiare e impostare la lingua inglese:

```
LC_MESSAGES=en_US
```

Adattamento per il supporto della lingua

Generalmente, per ottenere un fall back, i file delle categorie *Notizie* vengono archiviati solo nella directory della lingua (p.e. de). Se quindi LANG viene impostato su de_AT e se il file "Message" non è esistente sotto /usr/share/locale/de_AT/LC_MESSAGES, si ricorre a /usr/share/locale/de/LC_MESSAGES.

Con LANGUAGE è anche possibile determinare una "cascata" di fallback; p.e. per il bretone → francese o per il gallego → spangnolo → portoghese:

```
LANGUAGE="br_FR:fr_FR"
LANGUAGE="gl_ES:es_ES:pt_PT"
```

O – a seconda delle preferenze – utilizzare la variante norvegese "nynorsk" o "bokmål" (con ulteriore fallback su no):

```
LANG="nn_NO"
LANGUAGE="nn_NO:nb_NO:no"
```

o

```
LANG="nb_NO"
LANGUAGE="nb_NO:nn_NO:no"
```

Nel caso del norvegese, LC_TIME va trattato anche diversamente.

Problemi possibili

- Il punto delle cifre composte con 1.000 non viene riconosciuto. Probabilmente LANG si trova su de. Poichè la descrizione alla quale ricorre la glibc si trova in /usr/share/locale/de_DE/LC_NUMERIC, LC_NUMERIC deve venire impostato su de_DE.

Ulteriori informazioni:

- *The GNU C Library Reference Manual*, cap. "Locales and Internationalization"; contenuto nel pacchetto `glibc-info`, serie `doc`.
- Jochen Hein [Hei96], sotto il lemma "NLS".
- *German-Howto* di Winfried Trümper `file:/usr/share/doc/howto/en/html/German-HOWTO.html`
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, attuale sotto `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto* di Bruno Haible `file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

Supporto per programmi a 32 bit e a 64 bit in un ambiente a 64-bit

Nonostante SuSE Linux Enterprise Server sia disponibile per varie piattaforme a 64 bit, questo non significa necessariamente che tutte le applicazioni fornite a corredo sono state portate a 64 bit. SuSE Linux Enterprise Server supporta comunque applicazioni a 32 bit da eseguire in un ambiente a 64 bit. Questo capitolo vi mostra brevemente come si lascia realizzare tale supporto su piattaforme a 64 bit di SuSE Linux Enterprise Server.

Introduzione 154
Supporto runtime 154
Lo sviluppo di software 155
Il kernel 156

Introduzione

SuSE Linux Enterprise Server per le architetture a 64 bit ia64, ppc64, s390x, sparc64 ed AMD Hammep è stato concepito per eseguire applicazioni a 32 bit esistenti per la corrispondente architettura a 32 bit nell'ambiente a 64 bit e questo out of the box. Le rispettive architetture a 32 bit sono x86 per ia64, ppc per ppc64, s390 per s390x e x86 per AMD Hammer. Questo supporto vi permette di eseguire oggi le vostre applicazioni a 32 bit preferite invece di dover aspettare che vengano portate a 64 bit. L' attuale sistema ppc64 gira nella modalità a 32 bit, e vi consente di eseguire applicazioni a 64 bit.

Per quanto riguarda il supporto a 32 bit, diamo un'occhiata ai seguenti aspetti:

Supporto runtime Come è possibile lanciare applicazioni a 32 bit?

Supporto dello sviluppo Cosa bisogna fare per ottenere una applicazione a 32 bit che gira sia sull'architetture a 32 e 64 bit?

Kernel API Come è possibile che una applicazione a 32 bit giri sotto un kernel a 64 bit?

Supporto runtime

Nota

Conflitti tra la versione a 32 bit ed a 64 bit delle applicazioni
Se il vostro pacchetto è disponibile sia nella versione a 32 bit che a 64 bit, l'installazione parallela di entrambi le applicazioni causerà un conflitto. Dovete decidervi se installare la versione a 32 bit o a 64 bit.

Nota

Ogni applicazione necessità di un certo numero di librerie per funzionare correttamente. Purtroppo i nomi delle librerie a 32 bit e 64 bit sono identici, così bisogna differenziarli in qualche modo.

Le architetture a 64 bit, cioè ppc64, s390x, sparc64 ed AMD Hammer usano tutte lo stesso approccio: per assicurare la compatibilità con le versioni a 32 bit, le librerie a 32 bit si trovano precisamente nella stessa locazione come nell'ambiente a 32 bit. Per esempio, la versione a 32 bit di libc.so.6 si troverà sia in ambienti a 32 bit che in ambienti a 64 bit in `/lib/libc.so.6`.

Tutte le librerie a 64 bit e link object risiedono in directory chiamate `lib64`, vale a dire i link object a 64 bit che vi aspetterete di trovare in `/lib`, `/usr/`

`lib` e `/usr/X11R6` si trovano rispettivamente in `/lib64`, `/usr/lib64` e `/usr/X11R6/lib64`, per fare spazio alle librerie a 32 bit con lo stesso nome di base in `/lib`, `/usr/lib` e `/usr/X11R6/lib`.

Generalmente le sottodirectory delle directory link object che contengono solo dati indipendenti dalla dimensione del termine *non* sono stati spostati. Per esempio, troverete i font di X11 sotto `/usr/X11R6/lib/X11/fonts` come sempre.

Questa impostazione è conforme alla LSB (Linux Standards Base) e al FHS (Filesystem Hierachy Standard).

Per ia64 — e anche per la piattaforma a 64 bit di Alpha — le librerie native a 64 bit si trovano di default negli indirezzari `lib`, non vi è né `lib64` né `lib32`. Invece a64 gestisce il codice a 32 bit di x86 come emulazione. Un insieme di librerie di base viene installato nelle sottodirectory di `/usr/i386-linux`.

LD_LIBRARY_PATH e LD_PRELOAD

`LD_LIBRARY_PATH` e `/etc/ld.so.conf` sono combinati e contengono path per librerie sia a 32 che a 64 bit. Le applicazioni (almeno per PPC64) sono o a 32 o a 64 bit, e mai miste. Le applicazioni caricate cercano il tipo di libreria corretta (a 32 o a 64 bit) e saltano le librerie di un altro tipo. Se una applicazione necessita una libreria ma non riesce a trovare una libreria del tipo corretto nel path di ricerca, il caricamento dell'applicazione fallirà.

`LD_PRELOAD` e `/etc/ld.so.preload` può ottenere anche un misto di librerie a 32 e a 64 bit. Evitate path assoluti (che iniziano con "/") per il preload. Se applicazione richiede un path preload assoluto, generate uno shell script wrapper che imposta solo `LD_PRELOAD` per questa applicazione. Se utilizzate nomi di libreria relativi per un preload, assicuratevi che esistono sia librerie a 32 e a 64 bit (stesso nome ma directory diverse) e path per `LD_LIBRARY_PATH` e/o `/etc/ld.so.conf`.

Lo sviluppo di software

Tutte le architetture a 64 bit supportano lo sviluppo di oggetti a 64 bit. Solo il livello di supporto della compilazione a 32 bit dipende dalla architettura. Le diverse possibilità per la toolchain composta del GCC, la collezione di compiler GNU e i binutils che includono l'assembler as ed il linker ld sono:

Compilatore Biarch Con una toolchain per lo sviluppo biarch possono essere compilati sia oggetti a 32 bit che a 64 bit, di default vengono compilati oggetti a 64 bit. Speciali flag permettono di compilare oggetti a 32 bit. Il flag speciale per gcc è `-m32`, i flag per binutils dipendono dall'architettura, ma GCC fornirà i giusti flag al linker ed al assembler. Attualmente esiste una toolchain di sviluppo biarch per sparc64, (supporta anche lo sviluppo su sparc) e per AMD Hammer che supporta lo sviluppo dei set di istruzione per x86 e x86-64.

Nessun supporto SuSE Linux non supporta direttamente lo sviluppo di software a 32 bit su tutte le piattaforme. Se volete sviluppare applicazioni s390 o x86 rispettivamente su zSeries o su ia64, usate le corrispondenti versioni di SuSE Linux Enterprise Server a 32 bit.

32 bit di default La piattaforma PPC64 usa un compiler di default a 32 bit. Per compilare oggetti a 64 bit serve un cross compiler, i nomi dei tool iniziano con `powerpc64-linux-`, dunque nel caso di GCC avremo powerpc64-linux-gcc. Il compiler risiede in `/opt/cross/bin` che di default è nel path dell'utente. Le future versioni di SuSE Linux Enterprise Server Enterprise Server per PPC64 conterrano un compilatore biarch.

Considerate che i file header devono essere scritti in modo che non dipendano da una architettura particolare e che sia le librerie a 32 bit che a 64 bit dovrebbero avere un API (application programming interface) corrispondente ai file header installati. L'ambiente SuSE è stato concepito in questo modo, se eseguite un upgrade delle librerie dovete badare a questi aspetti.

Il kernel

I kernel a 64 bit per ia64, ppc64, s390x e AMD Hammer hanno sia una ABI (application binary interface) del kernel sia a 64 bit che a 32 bit, quest'ultima è identica alla ABI del corrispondente kernel a 32 bit. Questo significa che applicazioni a 32 bit possono interagire con il kernel a 64 bit nella stessa maniera come con il kernel a 32 bit.

Tenete presente che l'emulazione di chiamata di sistema a 32 bit del kernel a 64 bit non supporta parecchi API usati da programmi di sistema. Così è necessario che vi siano alcuni programmi di sistema, p. e. lspci o i programmi di amministrazione LVM, a 64 bit affinché il programma funzioni correttamente.

Un kernel a 64 bit riesce a caricare solo moduli di kernel a 64 bit compilati appositamente per il kernel. *Non* è possibile usare moduli di kernel a 32 bit.

Suggerimento

Alcune applicazioni necessitano propri moduli del kernel caricabili. Se volete usare una tale applicazione a 32 bit nell'ambiente a 64 bit, contattate il provider della applicazione e SuSE per accertarvi che la versione a 64 bit dei moduli del kernel caricabili e l'API del kernel a 32 bit per questo modulo siano disponibili.

Suggerimento

Il concetto di "boot"

Il caricamento e l'inizializzazione di un sistema Unix non sono semplici neanche per un amministratore esperto. Questo capitolo vi introduce brevemente il concetto di caricamento di SuSE Linux Enterprise Server e mette in pratica la sezione *Inizializzazione del sistema* della specificazione LSB (Versione 1.2); per più ampi dettagli sull'LSB, cfr. la sezione *Linux Standard Base (LSB)* a pagina 142.

Il programma init 160
I runlevel 160
Passaggio di runlevel 162
Gli script init 163
Il Runlevel Editor di YaST2 166
SuSEconfig, /etc/sysconfig e /etc/rc.config 167
Configurazione di sistema con l'editor Sysconfig di YaST2 168
Script e variabili: configurazione del sistema 169

Con la frase lapidaria "Uncompressing Linux...", il kernel assume il controllo di tutto l'hardware del sistema. Esso verifica ed imposta la console (ovvero la sezione del BIOS delle schede grafiche e del formato dello schermo), per poi leggere i parametri nel BIOS ed inizializzare le interfacce elementari della scheda madre. In seguito, i drive (che fanno comunque parte del kernel) esaminano l'hardware disponibile e lo inizializzano. Dopo la verifica delle partizioni ed il mount del file system root, il kernel avvia il programma init. Con init, viene a sua volta avviato il sistema vero e proprio, con rispettivi programmi di servizio e configurazione. Sarà il kernel a gestire tutto il sistema: esso controlla il tempo di elaborazione dei singoli programmi, mette a disposizione la memoria e gestisce l'accesso all'hardware.

Il programma init

Il programma init si occupa dell'inizializzazione corretta del sistema. Lo si potrebbe definire "il padre di tutti i processi" del sistema.

Tra tutti i programmi, init è quello che svolge un ruolo particolare: init viene avviato direttamente dal kernel ed è immune al segnale 9, con il quale può essere freddato ogni processo. Tutti gli altri processi vengono avviati da init stesso o da uno dei suoi processi "figli".

init si configura centralmente, tramite il file `/etc/inittab`, nel quale potrete definire i cosiddetti "runlevel" (vd. la sezione seguente, *I runlevel* in questa pagina) e fissare i servizi e daemon disponibili ad ogni livello. A seconda dei parametri su `/etc/inittab`, init avvia script differenti, che sono stati tutti riuniti nella directory `/etc/init.d` per motivi di praticità.

L'avvio del sistema (e, chiaramente, anche lo spegnimento) spetta quindi unicamente al processo di init. Il kernel può dunque essere visto come un "processo di fondo", il cui compito consiste nel gestire i processi avviati, assegnare loro un tempo di elaborazione e permetterne e controllarne l'accesso all'hardware.

I runlevel

Linux dispone di diversi *runlevel*, corrispondenti a diversi stati del sistema. Il runlevel standard sul quale si carica il sistema è fissato nel file `/etc/inittab`, alla voce `initdefault`. Normalmente, il valore standard è `3` o `5` (vd. tabella 8.1 a fronte). Alternativamente, potrete impostare il runlevel desiderato durante il caricamento (per esempio al boot prompt); il kernel passerà i parametri direttamente al processo init, senza elabolarli e modificarli.

Runlevel	Significato
0	Arresto del sistema (ingl. *System halt*)
S	Modo ad utente unico (ingl. *Single user mode*); dal boot prompt con tastiera americana
1	Modo ad utente unico (ingl. *Single user mode*)
2	Modo multiutente locale senza rete remota (ingl. *Local multiuser without remote network (es. NFS)*)
3	Modo multiutente locale pieno con rete (ingl. *Full multiuser with network*)
4	Libero (ingl. *Not used*)
5	Modo multiutente locale pieno con rete e KDM (standard), GDM o XDM (ingl. *Full multiuser with network and xdm*)
6	Riavvio del sistema (ingl. *System reboot*)

Tabella 8.1: *Lista dei runlevel disponibili su Linux*

Per passare ad un altro runlevel in un secondo momento, basta chiamare init con il numero del runlevel del caso; solo l'amministratore del sistema può modificare il runlevel.

Ad esempio, con il comando

```
root@terra:/ >  init 1
```

si passa nel *modo a utente unico* (ingl. *Single user mode*), che serve alla manutenzione ed amministrazione del sistema. Una volta che l'amministratore abbia completato le sue modifiche, immetterà

```
root@terra:/ >  init 3
```

per avviare il sistema sul normale runlevel, sul quale si trovano tutti i programmi necessari al funzionamento del sistema ed in cui si possono immettere tutti gli altri utenti.

La tabella 8.1 vi offre una sinossi dei runlevel disponibili. Vi consigliamo di non usare il runlevel 2 per un sistema che si trovi su una partizione `/usr` montata con l'NFS.

Da ciò consegue, in particolare, che potete arrestare il sistema anche con

```
root@terra:/ >  init 0
```

ovvero riavviarlo con

```
root@terra:/ >  init 6
```

L'installazione standard di SuSE Linux Enterprise Server imposta di solito il runlevel 5 come standard, in modo che l'utente si possa immettere direttamente tramite l'interfaccia grafica. Nel caso in cui l'impostazione del runlevel 5 sia stata resa impossibile da un intervento manuale, potrete sempre cambiarne la configurazione in seguito.

Per cambiare il runlevel da 3 a 5, assicuratevi che il X Window System sia già stato configurato correttamente; (Capitolo *Il sistema X Window* a pagina 33). Verificate il risultato delle vostre impostazioni con

```
root@terra:/ >  init 5
```

Se il sistema funziona come desiderate, passate su YaST2 e fissate il runlevel standard su 5.

Suggerimento

Modifiche personali di `/etc/inittab`
Degli errori su `/etc/inittab` potrebbero causare delle difficoltà di avvio del sistema. Siate estremamente cauti nel modificare queso file e assicuratevi di conservare sempre una copia del file originale intatto. Per riparare eventuali danni, provate ad inserire, al prompt di LILO, il parametro `init=/bin/sh`, e caricate il sistema in una shell. Da lì, ricostruite il file: `boot: linux init=/bin/sh`
Dopo il boot, ripristinate la copia di backup con il comando `cp`.

Suggerimento

Passaggio di runlevel

Generalmente, una modifica del runlevel significa che vengono eseguiti *gli script di arresto* del runlevel attuale, dove vengono terminati diversi programmi che vi si stiano svolgendo. Allo stesso tempo, vengono eseguiti gli *script di avvio* del nuovo runlevel ed avviata una serie di altri programmi.

Per meglio comprendere questo processo, osserviamo l'esempio del passaggio dal runlevel 3 al runlevel 5:

- L'amministratore (`root`) ordina al processo init di cambiare runlevel:

  ```
  root@terra:/ >  init 5
  ```

- init consulta il file di configurazione `/etc/inittab` e constata che lo script `/etc/init.d/rc` deve essere avviato con il nuovo runlevel come parametro.
- Ora, rc esegue tutti gli script di arresto dei runlevel per i quali non vi siano script di avvio nel nuovo runlevel. Nel nostro esempio, si tratta degli script contenuti nella directory `/etc/init.d/rc3.d` (il runlevel precedente era `3`) e che iniziano con la lettera `'K'`. Il numero che segue alla lettera `'K'` garantisce che venga mantenuta una determinata sequenza di esecuzione, dal momento che vi possono essere delle dipendenze tra un programma e l'altro.

Nota

Gli script di arresto iniziano sempre con la `'K'` (ingl. *kill*), mentre gli script di avvio iniziano con la `'S'` (ingl. *start*).

Nota

- Per ultimo, vengono eseguiti gli script di avvio del nuovo runlevel. Nel nostro esempio, questi script si trovano su `/etc/init.d/rc5.d` ed iniziano con `'S'`. Anche qui, si rispetta l'ordine prefissato dal numero dopo la lettera `'S'`.

Se passate nel runlevel in cui vi troviate già, init legge solo `/etc/inittab`, ne verifica la presenza di eventuali modifiche e, se necessario, adotta tutte le misure del caso (avviando, ad esempio, un `getty` su un'altra interfaccia).

Gli script init

Gli script su `/etc/init.d` si suddividono in due categorie:

- Script che vengono avviati direttamente da init: Questi script vengono attivati non solo durante il caricamento, ma anche in caso di spegnimento improvviso del sistema (per mancanza d'elettricità o quando l'utente prema la combinazione di tasti Ctrl + (Alt) + (Canc)).
- Script che vengono avviati indirettamente da init: Si dà questo caso quando si passi da un runlevel all'altro, laddove, normalmente, il primo script /etc/init.d/rc fa scattare gli altri nel giusto ordine.

Opzione	Significato
`start`	Avvia servizio
`stop`	Arresta servizio
`restart`	Arresta servizio e riavvialo, mentre il servizio è già in funzione; altrimenti, avvia servizio
`reload`	Ricarica configurazione del servizio senza fermarlo e riavvialo
`force-reload`	Ricarica configurazione del servizio se il servizio supporta questa operazione. Altrimenti fai `restart`
`status`	Mostra stato attuale

Tabella 8.2: *Tabella sinottica delle opzioni degli script init*

Tutti gli script si trovano su `/etc/init.d`, dove sono riuniti anche gli script per il passaggio di runlevel, con la differenza che questi ultimi vengono chiamati sempre da una delle sottodirectory di `/etc/init.d/rc0.d` a `/etc/init.d/rc6.d`, attraverso un link simbolico. Questo ne facilita l'uso ed evita di dover riprodurre gli script per poterli usare, ad esempio, su runlevel differenti. Dal momento che ogni script può fungere sia da script d'avvio che di arresto, essi devono poter leggere sia il parametro `start` che `stop`. Inoltre, gli script capiscono le opzioni `restart`, `reload`, `force-reload` e `status`; le funzioni delle opzioni sono riassunte nella tabella 8.2.

In uscita dal runlevel 3, viene avviato `/etc/init.d/rc3.d/K40network`; `/etc/init.d/rc` chiama lo script `/etc/init.d/network` con il parametro `stop`. In entrata nel runlevel 5, viene quindi avviato il medesimo script, questa volta, tuttavia, con il parametro `start`.

I link nelle singole subdirectory dei runlevel servono quindi solo a permettere l'assegnazione dei singoli script a determinati runlevel.

Per creare ed eliminare dei link, ci si serve di insserv (ovv. del link `/usr/lib/lsb/install_initd`) durante l'installazione o disinstallazione dei pacchetti del caso; cfr. pagina di manuale di `insserv` (`man 8 insserv`).

Segue una breve descrizione dei primi script di caricamento e spegnimento, nonché degli script di controllo:

`boot` viene eseguito allo start del sistema ed avviato direttamente da init. Non dipende dal runlevel di default e viene eseguito soltanto una volta: essenzialmente, vengono montati i file system `proc` e `devpts`, viene attivato il blogd (ingl. *Boot Logging Daemon*) e, dopo l'installa-

zione di un nuovo sistema o un'update, viene inizializzata una configurazione di base. A questo script viene attribuita anche la directory `/etc/init.d/boot.d`; tutti gli script di questa directory che comincino con la lettera `'S'` vengono automaticamente eseguito all'avvio del sistema. Vengono ora verificati i file system, vengono eliminati tutti i file superflui di `/var/lock` e viene configurata la rete per il dispositivo di loopback, se previsto. Allo stesso tempo, viene anche impostata l'ora del sistema. In caso di errori gravi nella verifica e nella riparazione automatica dei file system, l'amministratore del sistema dovrà inserire la root password e provvedere a risolvere manualmente il problema manualmente. Alla fine, viene eseguito localmente lo script boot.local.

`boot.local` Qui possono essere inseriti i parametri di tutti i processi che desideriate aggiungere al caricamento, prima che il sistema entri in un runlevel. Questa funzione può essere forse paragonata all'`AUTOEXEC.BAT` di DOS.

`boot.setup` Impostazioni fondamentali che devono essere mantenute nel passaggio dal modo a utente singolo ad un altro runlevel. In questo script vengono memorizzate le configurazioni di tastiera e console.

`halt` Questo script viene eseguito solo all'entrata nel runlevel 0 o 6. Per avviarlo, si usa `halt` o `reboot`, a seconda che si voglia che halt riavii o spenga il sistema.

`rc` Il primo script ad essere avviato nel passaggio tra runlevel. Esso esegue gli script di arresto del runlevel attuale e quelli di avvio del runlevel nuovo.

Potete anche aggiungere degli script vostri, servendovi della struttura predisposta su `/etc/init.d/skeleton`. Il formato preciso di uno script viene descritto nella bozza dell'LSB, dove vengono in particolare precisati sequenza e level di elaborazione dello script. Con `insserv`, dovrete ora creare dei link tra la directory `rc` del caso ed il nuovo script, in modo che lo script venga eseguito nel passaggio tra runlevel, come sopra descritto. Nello stesso documento vi viene spiegato come denominare i link. Per i dettagli tecnici, consultate la pagina di manuale di `init.d` (`man 7 init.d`) e la pagina di manuale di `insserv` (`man 8 insserv`). Come attrezzo di configurazione grafica per la creazione dei link, potete ricorrere al Runlevel Editor di YaST2; cfr. sezione *Il Runlevel Editor di YaST2* nella pagina seguente.

Attenzione

Script init personali

Degli errori negli script possono bloccare tutto il sistema. Siate pertanto molto cauti nello scriverli e verificatene prima il funzionamento nel modo multiutente, per quanto possibile. Per informazioni di base sull'uso degli script init dei runlevel, consultate la sezione *I runlevel* a pagina 160.

Attenzione

Il Runlevel Editor di YaST2

Questo modulo per esperti viene inizializzato dopo l'avvio del sistema. Nel dialogo successivo, vi viene mostrato il runlevel di default attuale. Questo "modo operativo" viene avviato dopo il boot del sistema. Su SuSE Linux Enterprise Server, si tratta normalmente del runlevel 5 (sistema multiutente pieno con rete e KDM, ovv. il login grafico). Molto buono è anche il runlevel 3 (modo multiutente pieno con rete). Con YaST2, potete qui impostare un altro runlevel di default; cfr. tabella 8.1 a pagina 161.

Con 'Modifica', passate ad una lista di tutti i servizi e daemon, che vi indica anche se questi siano attivi e per quali runlevel lo siano. Contrassegnando una delle righe con un clic del mouse, potete attivare le caselle dei runlevel '0', '1', '2', '3', '5', '6' e 'S' e così fissare i runlevel per i quali debba attivarsi il corrispondente servizio o daemon. Il runlevel 4 non è definito e resta a disposizione dell'utente per eventuali impostazioni personalizzate.

Con 'Avvia' e 'Arresta', decidete se fermare un determinato servizio. Con 'Attualizza', potete verificare lo stato attuale, nel caso in cui non sia già stato fatto automaticamente. 'Ripristinare valore di default' serve a ricaricare le impostazioni di default, ovvero quelle previste dall'installazione. 'Attiva servizio' appare solo se il servizio in questione non è attivo. 'Riportare tutti i servizi al valore default' ripristina le impostazioni del dopo-installazione. Salvate la configurazione con 'Fine'.

Attenzione

Modifica delle impostazioni del runlevel

Un'impostazione erronea dei servizi di sistema e dei runlevel può seriamente compromettere la funzionalità del vostro sistema. Prima di modificare delle impostazioni, vi preghiamo quindi di informarvi sulle loro possibili conseguenze.

Attenzione

SuSEconfig, /etc/sysconfig e /etc/rc.config

SuSE Linux Enterprise Server viene principalmente configurato tramite i file di configurazione che risiedono in `/etc/sysconfig`. `/etc/rc.config`, l'ex file di configurazione principale di SuSE Linux Enterprise Server è vuoto in modo da permettere ai vostri script di accedere alle vostre impostazioni e di applicare globalmente le vostre variabili.

I file di `/etc/sysconfig` vengono usati solo da alcuni script in situazioni ben determinate. In questo modo si assicura che le impostazioni della rete vengano elaborate solo dagli script della rete e non da altri.

Inoltre, molti altri file di configurazione del sistema vengono generati in dipendenza dai file di `/etc/sysconfig`, cosa a cui è preposto SuSEconfig. Ad esempio, dopo una modifica della configurazione di rete, viene ricreato il file `/etc/host.conf`, dal momento che esso varia a seconda del tipo di configurazione.

Ogni volta che modificate i suddetti file, dovete poi anche avviare SuSEconfig, per assicurare che le impostazioni vengano applicate a tutte le funzioni da esse interessate. Se usate YaST2, sarà lui ad avviare automaticamente SuSEconfig, attualizzando tutti i file che lo necessitino.

Questo sistema rende possibile rilevanti modifiche della configurazione del pc senza dover riavviare il computer. Nel caso di modifiche di ampia portata, potrebbe rendersi tuttavia necessario riavviare alcuni programmi per rendere effettivi i nuovi parametri.

I comandi

```
terra:~ #  rcnetwork stop
terra:~ #  rcnetwork start
```

riavviano i programmi di rete appena modificati. Come vedete, gli script init possono essere anche avviati manualmente.

Per configurare il sistema, consigliamo generalmente di procedere come segue:

- Portate il sistema in "single user mode" (runlevel 1):

  ```
  terra:~ #  init 1
  ```

- Eseguite le vostre modifiche dei file di configurazione. Servitevi di un texteditor o, meglio, dell'editor Sysconfig di YaST2; cfr. sezione *Configurazione di sistema con l'editor Sysconfig di YaST2* nella pagina successiva.

- Eseguite SuSEconfig per inserire le modifiche in diversi altri file di configurazione. Questo avverrà automaticamente, se avete usato YaST2 per impostare il runlevel.
- Riportate il sistema al runlevel precedente (nell'esempio, il 3):

```
terra:~ #  init 3
```

Questa procedura si rende chiaramente necessaria solo nel caso di modifiche di ampia portata (ad esempio, nella configurazione della rete). In casi più semplici non è neanche necessario che l'amministratore passi al "single user mode"; tuttavia, assicuratevi che tutti programmi interessati dalle vostre modifiche vengano riavviati.

Suggerimento

Potete disattivare la configurazione automatica *in tutto il sistema* con SuSEconfig, impostando la variabile ⟨*ENABLE_SUSECONFIG*⟩ di `/etc/sysconfig/suseconfig` su `no`. Per poter continuare ad usare il supporto all'installazione, la variabile ⟨*ENABLE_SUSECONFIG*⟩ dovrà tuttavia essere impostata su `yes`. Potete anche deattivare singolarmente alcune parti dell'autoconfigurazione.

Suggerimento

Configurazione di sistema con l'editor Sysconfig di YaST2

Nella directory `/etc/sysconfig`, troverete tutti i file contenenti le impostazioni di SuSE Linux Enterprise Server più importanti (prima, queste impostazioni venivano gestite centralmente, nel file `/etc/rc.config`) L'editor Sysconfig di YaST2 vi presenta tutte le possibilità di impostazione. I valori possono essere modificati e poi inseriti nei singoli file di configurazione. Le modifiche manuali non sono, tuttavia, generalmente necessarie, dal momento che i file vengono attualizzati automaticamente ogni volta che venga installato un pacchetto o impostato un servizio.

Attenzione

Modifiche dei file `/etc/sysconfig/*`

Tutte le modifiche di `/etc/sysconfig/*` hanno profonde conseguenze per tutto il sistema. Prima di effettuare una modifica, vi preghiamo pertanto di informarvi sulle sue possibili conseguenze e di assicurarvi che esse non compromettano la funzionalità del vostro pc.

Attenzione

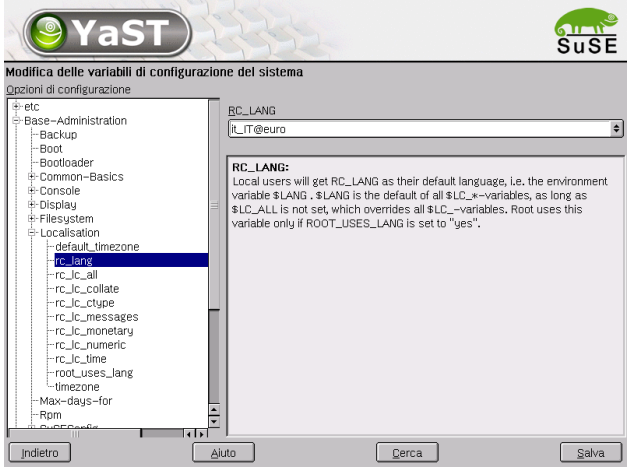


Figura 8.1: *YaST2: Configurazione dell'editor sysconfig*

Script e variabili

In quel che segue, descriveremo brevemente *alcuni* parametri del sistema e le loro rispettive impostazioni. Nel caso in cui *non* vi serviate di YaST per modificare il file di configurazione di `/etc/sysconfig`, non dimenticate di usare, per descrivere un parametro vuoto, due doppie virgolette consecutive (ad esempio ⟨*KEYTABLE=""*⟩) e di chiudere i parametri che contengano una riga vuota tra doppie virgolette. Per variabili di una sola parola non sono necessarie virgolette.

Nota

Variabili specifiche di piattaforma su /etc/sysconfig
Le variabili che vi presentiamo qui ed i file di /etc/sysconfig sono concepiti per essere il minimo comune denominatore di tutte le piattaforme supportate. Alcune delle variabili che menzioniamo potrebbero non esistere sulla vostra piattaforma o essere usate solo in tipologie specifiche di piattaforme. Vi preghiamo di consultare la documentazione dei file /etc/sysconfig.

Nota

Impostazioni nei file di /etc/sysconfig

3ddiag Per 3Ddiag.

SCRIPT_3D="switch2mesasoft"
Impostare lo script che crei i necessari link simbolici per le biblioteche ed estensioni OpenGL giuste. Tra i valori possibili per gli script su /usr/X11R6/bin vi sono:

no – Non eseguire alcuno script

switch2mesasoft – Emulazione del software Mesa (funziona con tutte le schede grafiche)

switch2mesa3dfx – Mesa/Glide

switch2nvidia_glx – XFree86 4.x/NVIDIA_GLX (NVIDIA_GLX/NVIDIA_kernel)

switch2xf86_glx – XFree86 4.x/DRI

3Ddiag vi aiuta a trovare i valori giusti .

SuSEfirewall2 Attivazione del firewall; cfr. descrizione su pacchetto SuSEfirewall2.

amavis Attivazione dell'antivirus AMaViS su Sendmail o Postfix.

USE_AMAVIS="yes"
Per attivare AMaViS. SuSEconfig si occuperà della configurazione di Sendmail o Postfix più adeguata. Per maggiori dettagli, consultate README.SuSE del pacchetto AMaViS.

apache Configurazione del webserver Apache. Questa configurazione si limita solo alle impostazioni di default o indispensabili per il funzionamento di Apache. Per tutte le altre variabili o moduli e le loro funzioni, vi preghiamo di leggere la documentazione di Apache, che potrete installare con il pacchetto apache-doc di YaST2 o che troverete su Internet ai seguenti URL:

http://httpd.apache.org/docs/ e http://modules.apache.org

HTTPD_PERFORMANCE="slim"
Per fissare il numero di client del vostro server. Potete scegliere tra le classi "slim", "mid", "thick" e "enterprise". SuSEconfig adatta poi i MinSpareServers, i MaxSpareServers, gli StartServers ed i MaxClients nella configurazione di Apache /sbin/conf.d/SuSEconfig.apache.

HTTPD_START_TIMEOUT="2"
Per fissare il numero di secondi entro il quale lo script di avviamento, verificate che il processo http sia stato avviato senza errori. Se usate mod_ssl ed il vostro certificato SSL è protetto da password, aumentate questo valore.

HTTPD_SEC_ACCESS_SERVERINFO="no"
Questa impostazione attiva i moduli mod_status e mod_info, che vi informano rispettivamente sullo stato, la prestazione e la configurazione del vostro server.

HTTPD_SEC_SAY_FULLNAME="no"
Quali informazioni comunicare all'esterno attraverso il server, in forma di una nota a piè di pagina nei documenti generati dal server stesso (es. comunicazioni d'errore)? Potete scegliere tra yes, se desiderate inviare il numero di versione ed il nome del server, no per non mandare alcuna informazione e email, se desiderate inviare numero di versione, nome e mailto: all'amministratore del server. Questa variabile è sempre connessa alla direttiva ServerSignature di Apache.

HTTPD_SEC_SERVERADMIN=""
Inserite qui l'indirizzo di email dell'amministratore del server. Se avete impostato la variabile ⟨*HTTPD_SEC_SAY_FULLNAME*⟩ su yes, questo dato viene inoltrato all'esterno. Se lasciate la variabile vuota, essa viene usata come indirizzo di email webmaster@$HOSTNAME. ⟨*HOSTNAME*⟩ (il nome dell'host del server per intero) viene fissato nel file /etc/HOSTNAME. ⟨*HTTPD_SEC_SERVERADMIN*⟩ corrisponde alla direttiva ServerAdmin di Apache. Le direttive ServerAdmin negli statement VirtualHost non vengono qui modificate dalla vostra impostazione, esattamente come non viene toccata la configurazione degli SSL Virtual Host.

HTTPD_SEC_PUBLIC_HTML="yes"
Volete rendere accessibili le directory public_html della home directory degli utenti? Se la risposta è yes, eseguite le altre impostazioni su /etc/httpd/suse_public_html.conf.

HTTPD_CONF_INCLUDE_FILES=""
Indicate i file, divisi da uno spazio, che devono essere assunti da `/etc/httpd/httpd.conf`. In questo modo, potrete, per esempio, creare nuovi `VirtualHost` statement senza dover modificare anche `/etc/httpd/httpd.conf`. Fintato che SuSEconfig non constati alcuna modifica di `/etc/httpd/httpd.conf` con il meccanismo di somme MD5 `/etc/httpd/httpd.conf`, questo file non deve venire toccato dalla configurazione di Apache.

HTTPD_AWSTATS_COMBINED_LOG="yes"
Desiderate che Apache crei un logfile a parte, che venga esaminato da awstats (ingl. *Advanced Web Statistics*)?

HTTPD_DDT="yes"
Per attivare il DDT Admin CGI. Lo potete usare per creare e gestire server account su un DDT (ingl. *Dynamic DNS Tools*) locale.

MAILMAN_APACHE="yes"
Desiderate che il Webfrontend Mailman venga attivato per la gestione di mailing list?

HTTPD_SEC_MOD_MIDGARD="yes"
Attivazione del modulo `midgard`. Midgard è un Open Source Content Management System.

HTTPD_SEC_MOD_PERL="yes"
Attivazione del modulo `mod_perl`.

HTTPD_SEC_MOD_PHP="yes"
Attivazione del modulo `mod_php`.

HTTPD_SEC_MOD_PYTHON="yes"
Desiderate attivare il modulo Python di Apache? Il valore di default è `yes`.

HTTPD_SEC_NAGIOS="yes"
Per permettere l'accesso all'interfaccia web Nagios. Si configura su `/etc/httpd/nagios.conf`.

HTTPD_SEC_MOD_SSL="no"
Per attivare il modulo SSL. Il valore di default è `no`, dal momento che sono necessarie un paio di impostazioni preliminari prima che l'SSL funzioni perfettamente. Certificate il vostro server. Per creare un certificato di prova, passate al modo root ed immettete i seguenti comandi nell'ordine seguente:

```
cd /usr/share/doc/packages/mod_ssl
./certificate.sh
```

Impostate la variabile ⟨*ServerName*⟩ di `VirtualHost _default_:443` della directory `httpd.conf` sul nome completo del server (ingl. *Fully Qualified Domain Name*) (vd. ⟨*HOSTNAME*⟩ `/etc/HOSTNAME`).
Aumentate il valore della variabile ⟨*HTTPD_START_TIMEOUT*⟩, se il certificato server è protetto da una password (vedi sopra).

ZOPE_PCGI="no"
Volete elaborare le richieste del programma Zope attraverso l'interfaccia PCGI di Apache? Allora non modificate il valore di default di questa variabile `no`, e avviate Zope come server Web nella modalità stand-alone. Selezionate qui `yes`, per poter utilizzare PCGI dovete aver installato Apache. Sotto `/etc/sysconfig/zope` trovate ulteriori opzioni.

ZOPE_KEEP_HOMES="yes"
Se le richieste di Zope dovranno essere elaborate attraverso apache-pcgi e ⟨*ZOPE_KEEP_HOMES*⟩ avere il valore `yes`, le directory home degli utenti veranno gestiti da Apache.

argoups Configurare argoups. Questo pacchetto permette di spegnere il sistema in modo controllato attraverso un demone particolare, qualora l'unità di continuità (USV) segnala una mancanza temporanea della corrente.

ARGO_TYPE="local"
Immettete qui il tipo di connessione verso il sistema da controllare. Se volete "controllare da remoto" un sistema, immettete il nome del sistema da controllare in ⟨*ARGO_REMOTESERVER*⟩.

ARGO_REMOTESERVER=""

ARGO_TTY="/dev/ttyS0"
Attraverso quale porta seriale è stata realizzata la connessione ad ArgoUPS?

ARGO_USERTIME="2"
Dopo quanto tempo (minuti) dalla mancanza di corrente debba venire eseguito lo script da ⟨*ARGO_USERFILE*⟩?

ARGO_USERFILE="/usr/sbin/argoblackout"

ARGO_SHUTDOWN="8"
Dopo quanto tempo deve essere eseguito lo shutdown?

argus Server per Argus (monitor di rete).

ARGUS_INTERFACE="eth0"
L'interfaccia da controllare da Argus.

ARGUS_LOGFILE="/var/log/argus.log"
Il log-file Argus. Questo file può raggiungere dimensioni notevoli!

autofs Questo demone permettete di montare automaticamente sia directory che possono essere indirizzate via NFS che directory locali (lettore CD-ROM, dischetti etc.).

AUTOFS_OPTIONS=""
Opzioni di autofs, per esempio "`--timeout 60`". Con l'opzione `-timeout` viene stabilito dopo quanto tempo (secondi) le directory debbano essere smontate (ingl. *unmount*) automaticamente.

autoinstall AutoYaST2 L'Auto-Installer di YaST2.

REPOSITORY="/var/lib/autoinstall/repository"
Archivio per i "profili". Si tratta di file di controllo contenenti le descrizioni di configurazione per gli host da installare.

CLASS_DIR="/var/lib/autoinstall/classes"
Durante la creazione di profili/file di controllo per complessi scenari di installazione con tanti host, potete semplificare il tutto definendo delle classi che rappresentano diversi tipi e/o gruppi di host. YaST2 li archivierà sotto `/var/lib/autoinstall/classes`.

PACKAGE_REPOSITORY=""
Questa directory contiene dati di installazione/pacchetti per SuSE Linux Enterprise Server.

backup Copie del RPM database.

RPMDB_BACKUP_DIR="/var/adm/backup/rpmdb"
Stabilisce dove cron.daily debba scrivere i backup del RPM database; se non desiderate dei backup settate questa variabile su `""` .

MAX_RPMDB_BACKUPS="5"
Stabilisce il numero dei backup del RPM database.

RCCONFIG_BACKUP_DIR="/var/adm/backup/rpmdb"
Nella directory qui specificata cron.daily archivia i backup del vostro `/etc/rc.config` e dei file che si trovano sotto `etc/sysconfig/`. Il backup dei file modificati viene realizzato alla prossima esecuzione di cron.daily. Se non desiderate dei backup, settate la variabile su `""` .

MAX_RCCONFIG_BACKUPS="5"
Qui stabilite il numero dei backup da creare dei file sotto `/etc/sysconfig` e di `/etc/rc.config`.

clock Impostazione dell'orario.

GMT=""
Se l'orario del vostro sistema è impostato su GMT (*Greenwich Mean Time*), settate questa variabile su `-u`, altrimenti impostatela su `--localtime`. Questa impostazione consente il cambio automatico tra l'ora legale e solare.

TIMEZONE=""
Il vostro fuso orario o il fuso orario su cui avete impostato il computer. Questa impostazione è importante anche per il cambio automatico tra ora legale e solare. Così viene impostato `/usr/lib/zoneinfo/localtime`.

console Impostazione per la console.

FB_MODULES=""
Volete integrare dei moduli driver del frame buffer nel vostro kernel? Prima di decidervi dovete considerare che le vostre impostazioni non funzionano se vesafb è già abilitato. Inoltre è preferibile compilare il supporto framebuffer direttamente nel kernel, poichè alcuni driver XFree86 (soprattutto della serie XFree86-4.x) causano dei problemi con il frame buffer nel modo testo.

FBSET_PARAMS=""
Se il vostro kernel supporta il frame buffer (o se tale supporto si lascia realizzare caricando un modulo), vorrete modificare la risoluzione od altri parametri. Impostate i parametri con fbset (Per i dettagli: `man fbset` e/o `fbset -h`).

Attenzione

Impostare i parametri del frame buffer
Le impostazioni possibili dipendono dalla vostro hardware e software. Se commettete degli errori, potreste danneggiare il vostro monitor. Dunque considerate che vesafb non supporta (ancora) il cambio della modalità display

Non selezionate modalità display non supportate dal vostro monitor.

Attenzione

CONSOLE_FONT=""
Il font che viene caricato per la console al momento dell'avvio. Non tutti i font supportano per esempio vocali accentuati o altri caratteri a 8 bit! Le impostazioni aggiuntive sono: ⟨*CONSOLE_SCREENMAP*⟩, ⟨*CONSOLE_UNICODEMAP*⟩ e ⟨*CONSOLE_MAGIC*⟩.

CONSOLE_UNICODEMAP=""
Alcuni font sono sprovvisti di proprie Unicode Map. Indicate qui esplicitamente l'Unicode Mapping da voi desiderato. Il file si trova sotto `/usr/share/kbd/unimaps/`. Normalmente comunque questa opzione non è necessaria.

CONSOLE_SCREENMAP=""
Il font da voi utilizzato dever essere convertito nel set di caratteri Unicode? Immettete qui lo screen map adatto. Gli screen map risiedeno sotto `/usr/share/kbd/consoletrans/`.

CONSOLE_MAGIC=""
Eventualmente la console deve essere inizializzata - a secondo del font utilizzato - con ⟨*CONSEOLE_MAGIC*⟩ Di solito comunque qui non si devono apportare delle modifiche.

SVGATEXTMODE="80x25"
Con le schede SVGA il pacchetto relativo `svgatext` consente di impostare risoluzioni di testo più elevate (fino a 160x60). Questa variabile ottiene un valore valido dal `/etc/TextConfig`. Adattate questo file corrispondentemente alle caratteristiche della vostra scheda grafica. In `/usr/share/doc/packages/svgatext` viene spiegato il modo di farlo. L'impostazione di default per ⟨*SVGATEXTMODE*⟩ è di"80x25". Risoluzioni SVGATextMode vengono usate nei runlevel 1,2,3 e 5.

cron Manutenzione quotidiana del sistema.

Il demone cron avvia automaticamente ad orari prestabiliti certi programmi. Si consiglia assolutamente di attivare il demone cron su computer che sono accesi 24 ore su 24. Il demone AT rappresenta un'alternativa o un completamento.

Nota

Esistono una serie di impostazioni di sistema che richiedono l'avvio ad intervalli regolari di determinati programmi, così il demone Cron dovrebbe essere abilitato su ogni sistema.

Nota

MAX_DAYS_IN_TMP="0"
Ogni giorno viene controllato se nelle directory `tmp` (vedi ⟨*TMP_DIRS_TO_CLEAR*⟩) vi sono dei file a cui non si accede ormai da un periodo superiore a quello indicato (in giorni). Se in questa directory vi è un file che non è stato usato per un periodo superiore a quello indicato, il file viene cancellato.

Questo meccanismo si lascia disattivare con "" o `0` (default). Questa variabile va impostata quando sono più utenti ad usare il sistema per evitare uno straripare delle directory `tmp`.

`TMP_DIRS_TO_CLEAR="/tmp /var/tmp"`
Indicazione delle directory all'interno dei quali si devono cercare ogni giorno file "datati" da cancellare; cfr. ⟨*MAX_DAYS_IN_TMP*⟩.

`OWNER_TO_KEEP_IN_TMP="root"`
I file degli utenti del sistema qui riportati non devono essere cancellati dalle directory `tmp`(vd. ⟨*TMP_DIRS_TO_CLEAR*⟩), anche se non vi è stato un accesso oltre al periodo indicato.
Attenzione: Se ⟨*CLEAR_TMP_DIRS_AT_BOOTUP*⟩ sta su `yes`, questa registrazione *non* viene considerata!

`CLEAR_TMP_DIRS_AT_BOOTUP="no"`
Settate queste variabili su `yes`, se volete cancellare (`rm -fr`) tutti i file e sottodirectory nelle directory temporanee specificate in ⟨*TMP_DIRS_TO_CLEAR*⟩.
Attenzione: Se questa variabile è impostata su `yes` le registrazioni in ⟨*OWNER_TO_KEEP_IN_TMP*⟩ *non* presi in considerazione; tutti i file saranno cancellati!

`DELETE_OLD_CORE="no"`
I *corefiles* sono immagini del fabbisogno di memoria dei programmi che sono stati interrotti a causa dell'avvenuta violazione della protezione della memoria; queste immagini sono utile nel localizzare errori. Qui avete la possibilità di impostare che i vecchi corefile vengano regolarmente individuati e automaticamente cancellati. Contemporaneamente dDovrà essere installato il pacchetto pacchetto `findutils-locate` e ⟨*RUN_UPDATEDB*⟩ essere impostato su `yes`.

`MAX_DAYS_FOR_CORE="7"`
Stabilisce il limite massimo della durata di vecchi corefile (in giorni), superato il quale vengono cancellati automaticamente.

`REINIT_MANDB="yes"`
Per stabilire se i database delle pagine di manuale (mandb und whatis) di cron.dailyvanno ricreati giornalmente.

`DELETE_OLD_CATMAN="yes"`
Si devono cancellare le vecchie pagine di manuale preformattate in `/var/catman`?

`CATMAN_ATIME="7"`
Per quanti giorni si devono conservare le pagine di manuale preformattate prima di cancellarle?

dhcpd Configurazione del server DHCP

DHCPD_INTERFACE="eth0"
Interfaccia/e sulla/e quale/i il server DHCP deve mettersi in ascolto.

DHCPD_RUN_CHROOTED="yes"
dhcpd deve girare in una "chroot jail"? Leggete il README.SuSE su dhcp che trovate sotto `/usr/share/doc/packages/dhcp/README.SuSE`.

DHCPD_CONF_INCLUDE_FILES=""
Il file `dhcpd.conf` può contenere l'istruzione `include`. Indicate in ⟨*DHCPD_CONF_INCLUDE_FILES*⟩ tutti i file che volete includere. In tal modo *tutti* i vostri file `.conf` e `/etc/dhcpd.conf` vengono copiati nella directory chroot (`\$chroot/etc/`)

DHCPD_RUN_AS="nobody"
Stabilite come quale tipo utente debba venire avviato dhcpd. Se questa variabile rimane vuota oppure se immettete `root`,dhcpd viene avviato come `root`. Con `nobody` si avvia come `nobody` del gruppo `nogroup`.

DHCPD_OTHER_ARGS=""
Qui potete dare a dhcpd ulteriori argomenti (vd. `man dhcpd`).

dhcrelay Configurazione del DHCP Relay Agent. Funge da "intermediario" tra sottoreti con o senza un proprio server DHCP. Inoltra richieste DHCP (e Bootp) provenienti da una sottorete senza un server proprie ad un o più server DHCP nella rete e ne trasmette la risposta.

DHCRELAY_INTERFACES=""
Interfacce sulle quali il DHCPR Relay Agent deve mettersi in ascolto. Separete le registrazioni con uno spazio.

DHCRELAY_SERVERS=""
A quali server DHCP può rivolgersi il DHCP relay agent? Immettete qui un o più server separati da uno spazio.

displaymanager Configurare il display manager.

DISPLAYMANAGER=""
Questa variabile stabilisce quale display manager usare per entrare nel sistema ("login"). Valori possibili sono `console`, `xdm` (display manager tradizionale di X Window System), `kdm` (display manager di KDE), `gdm` (display manager di GNOME) o `wdm` (il display manager "WINGs").

DISPLAYMANAGER_REMOTE_ACCESS="no"
Volete consentire l'accesso da remoto al vostro display manager? L'impostazione di default è `no`.

DISPLAYMANAGER_STARTS_XSERVER="yes"
Il display manager deve lanciare un X server locale? Se volete permettere solo un accesso da remoto, questa variabile va impostata su no.

KDM_SHUTDOWN="auto"
Qui potete stabilire chi possa eseguire lo shutdown del sistema in kdm. Valori possibili sono `root`, `all`, `none`, `local` ed `auto`.

KDM_USERS=""
Immettete l'elenco degli utenti separati da uno spazio per i quali in kdm devono essere visualizzate le icone. Se non immettete delle registrazioni vostre, vengono utilizzate le impostazioni di default del sistema.

KDM_BACKGROUND=""
Qui potete scegliere lo sfondo per kdm angeben.

KDM_GREETSTRING=""
Desiderate un benvenuto particolare di kdm?

dracd Impostazioni per il demone di dracd e il Mail Relaying attraverso "POP-before SMTP."

DRACD_RELAYTIME="5"
Postfix mantiene per un determinato lasso di tempo l'indirizzo IP di un host autenficato sul server POP, e consente l'invio di e-mail appunto da questo host. Dopo tale periodo la registrazione viene cancellata e una nuova autenticazione si rende necessaria. Il tempo viene indicato in minuti.

DRACD_DRACDB="/etc/postfix/dracd.db"
Qui trovate `dracdb`.

dvb Scheda DVB

DVB_SOUND_CHIP="ti"
Selezionare il sound chip sulla scheda DVB; `ti` o `crystal`.

hardware Impostazioni dell'hardware.

DEVICES_FORCE_IDE_DMA_ON=""
Attivare il DMA nei dispositivi menzionati.

DEVICES_FORCE_IDE_DMA_OFF=""
Disattivare il DMA nei dispositivi menzionati.

hotplug Impostazioni Hotplug.

HOTPLUG_DEBUG="default"
Con questa variabile controllate il numero dei messaggi (di errore) che il servizio hotplug segnala a syslog. `default`, `""` , o `no` comportano un numero moderato di messaggi, `off` "ammutulisce" l'hotplug e `verbose` o `yes` trasmettono inoltre alcuni messaggi di debug. `max` comporta che `syslog` viene "sommerso" di messaggi.

HOTPLUG_START_USB="yes"
Qui potete avviare o fermare l' USB Hotplug.

Nota

Disattivare l'USB Hotplug
Se disattivate l'USB Hotplug e avete caricato i dispositivi di input USB come modulo, la vostra tastiera non reagirà se cercate di digitare, poiché in tal modo disattivate anche il supporto della tastiera.

Nota

HOTPLUG_USB_HOSTCONTROLLER_LIST="usb-uhci uhci usb-ohci ehci-hcd"
Qui stabilite la sequenza di "probing"dei driver del controller dell'host driver.

HOTPLUG_USB_MODULES_TO_UNLOAD="scanner"
Questi moduli vengono rimossi con un USB "remove". Con certi componenti hardware si consiglia di reinizializzare il dispositivo.

HOTPLUG_USB_NET_MODULES="pegasus usbnet catc kaweth CDCEther"
Se uno di questi moduli viene caricato nella/dalla memoria, il sistema presume che si tratti di un dispositivo di rete e crea la descrizione hardware per il seguente cosiddetto "net event".

HOTPLUG_START_NET="yes"
Attivare/disattivare il NET Hotplug Event Handling.

HOTPLUG_NET_DEFAULT_HARDWARE=""
Se hotplug riconosce autonomanente quale tipo di hardware si cela dietro l'interfaccia di rete, vengono create con USB o PCI Hotplug Events descrizioni hardware, che vengono letti durante il NET Event. L'aggiunta contemporanea di diversi dispositivi hotplug può condurre a cosiddette race conditions. Se il rilevamento automatico di nuovi dispositivi non funziona, all'inizializzazione di if{up,down} viene analizzato il contenuto di ⟨*HOTPLUG_NET_DEFAULT_HARDWARE*⟩. Immettete qui cosa utilizzate come NIC (ingl. *Network Interface Card*): `pcmcia`, `usb` o `firewire`.

HOTPLUG_NET_TIMEOUT="8"
Indicate per quanti secondi si debba attendere ad una descrizione hardware di un USB o PCI Hotplug Event. Se immettete `0`, viene analizzata automaticamente ⟨*HOTPLUG_NET_DEFAULT_HARDWARE*⟩. L'impostazione di default di otto secondi considera il tempo necessario di alcune schede di rete PCMCIA.

HOTPLUG_START_PCI="yes"
Attivare/disattivare il PCI Hotplug Event Handling.

HOTPLUG_PCI_MODULES_NOT_TO_UNLOAD=""
I seguenti moduli non devono venire caricati dalla memoria durante un "PCI remove Event".

intermezzo Impostazioni del file system Intermezzo.

EXCLUDE_GID="63"
Indicate quale gruppo deve essere escluso dalla replica.

irda IrDA è l'interfaccia ad infrarossi di alcuni notebook.

IRDA_PORT="/dev/ttyS1"
Per il momento viene supportato solo il modo seriale (UART [SIR]) nella configurazione standard. Nel setup del BIOS-Setup potete vedere che tipo di porta seriale venga usata. Se disponete di un chip set FIR supportato, stabilite il modulo del kernel relativo(per esempio `toshoboe`). Bisogna attivare FIR innanzitutto nelle impostazioni BIOS. A volte può verificarsi la necessità di deattivare la porta seriale con `setserial /dev/ttyS<x> uart none`.

isdn/ Gli script rilevanti per ISDN.

ispell Controllo ortografico.

ENGLISH_DICTIONARY="system american british"
SuSEconfig.ispell amministra un link simbolico dal dizionario "inglese" verso `american` o `british`. Se è installato sia ispell-american che ispell-british, il link punterà su ⟨*ENGLISH_DICTIONARY*⟩. Il valore `system` indica la lingua di default del sistema (stabilita in `/etc/sysconfig/language` sotto ⟨*RC_LANG*⟩), se si tratta di una delle due lingue inglesi. Altrimenti `system` non ha alcun effetto. Un link simbolico punterà sul dizionario installato dell'elenco installato come primo.

java Impostazioni per la configurazione Java

CREATE_JAVALINK="yes"
SuSEconfig crea per voi i link `/usr/lib/java` e `/usr/lib/jre` verso i relativi JDK (ingl. *Java Development Kit*) e JRE (ingl. *Java Runtime Environment*), se impostate il valore di questa variabil su `yes`. Se preferite la configurazione a mano impostate ⟨*CREATE_JAVALINK*⟩ su `no`.

JAVA_JRE_THREADS_TYPE="green"
Configurazione del pacchetto `java-jre`. Se desiderate Multithreading *vero*, impostate questa variabile su `native` che è utile per esempio in combinazione con sistemi SMP.

JAVA_THREADS_TYPE="green"
Configurazione del pacchetto `java`. Se desiderate Multithreading *vero*, impostate questa variabile su `native` che è utile per esempio in combinazione con sistemi SMP.

joystick Impostazioni della configurazione del Joystick.

GAMEPORT_MODULE_0=""
Nome del modulo del gameport, per esempio `ns558` per un gameport più datato.

JOYSTICK_MODULE_0=""
Di solito `analog`.

JOYSTICK_MODULE_OPTION_0=""
Per esempio "`js=gameport`" per `analog`.

JOYSTICK_CONTROL_0=""
Per esempio `yes`.

JOYSTICK_CONTROL_PORT_0=""
Le schede audio del tipo ens1371 hanno bisogno qui dell'indirizzo della porta; solitamente `0x200`.

kernel Kernel.

INITRD_MODULES=""
I nomi dei moduli che vanno aggiunti al initial ramdisk con `mk_initrd`. (per esempio driver per controller SCSI, LVM o ReiserFS) .

SHMFS=""
Qui stabilite il parametro per la quantità di memoria destinato il mount del filesystem shmfs. Di solito il kernel utilizza qui il 50% della memoria disponibile che comunque a volte non è sufficiente in relazione al setup specifico.

keyboard Impostazione della tastiera.

KEYTABLE="de-latin1-nodeadkeys"
Definisce la mappatura della tastiera. Se utilizzate una tastiera americana questa variabile può essere lasciata vuota.

KBD_RATE="24.0"
Determina la velocità di ripetizione dei tasti automatica. E' possibile stabilere una frequenza da due fino a 30 volte al secondo. Questa impostazione funziona solo se determinate contemporaneamente anche la velocità di reazione dei tasti. (cfr. ⟨*KBD_DELAY*⟩)

KBD_DELAY="500"
Valori possibili: `250`, `500`, `750` e `1000`. Impostate qui la velocità di reazione dei tasti, sulla quale si baserà anche la funzione di ripetizione. Il valore è espresso in millisecondi, ma il meccanismo di regolazione non è molto preciso. Dovete impostare anche ⟨*KBD_RATE*⟩!

KBD_NUMLOCK="bios"
Con `no` non viene attivato il tasto (NumLock) al boot. Altre possibili impostazioni sono sono `yes`, `""` o `bios` per impostazioni BIOS.

KBD_SCRLOCK="no"
Attivare (SrollLock)?

KBD_CAPSLOCK="no"
Non accendere (CapsLock) durante l'avvio del sistema.

KBD_DISABLE_CAPS_LOCK="no"
Intendete spegnere (CapsLock) e volete che agisca a guisa del tasto (Shift)?

KBD_TTY="tty1 tty2 tty3 tty4 tty5 tty6"
(NumLock), (CapsLock) e (ScrollLock) possono venire ristretti a determinati TTY; "" sta per tutti TTY.

COMPOSETABLE="clear winkeys shiftctrl latin1.add"
Qui stabilite quali "Compose Table" caricare. "Compose table" vi permettono di digitare caratteri speciali (accenti, simboli di valuta etc.), non direttamente presenti sulla tastiera attraverso una particolare combinazione di tasti. Sotto `/usr/share/doc/packages/kbd/README.SuSE` trovate una spiegazione dettagliata.

language Impostazioni di lingua e luogo (locali).

RC_LANG="de_DE@euro"
Imposta `LANG` per locale; qui può essere indicato un valore per l'utente locale. Questo valore è determinante fino a che non vengono impostate variabili ⟨*RC_LC_**⟩ particolari.
Possibili variabili `sysconfig`: ⟨*RC_LC_ALL*⟩ (possibilità di sovrascrivere `LC_*` e anche `LANG`!), ⟨*RC_LC_MESSAGES*⟩, ⟨*RC_LC_CTYPE*⟩,

⟨*RC_LC_MONETARY*⟩, ⟨*RC_LC_NUMERIC*⟩, ⟨*RC_LC_TIME*⟩ e ⟨*RC_LC_COLLATE*⟩.
Cfr. sezione *Adattamenti locali – I18N/L10N* a pagina 149.

ROOT_USES_LANG="ctype"
Le impostazioni di locale devono essere applicate anche a `root`? `ctype` significa che qui viene utilizzato un valore di ⟨*LC_CTYPE*⟩.

locate La banca dati locate trova velocemente dei file nel sistema. – Viene aggiornata a secondo dei casi poco dopo l'avvio del sistema se il computer *non* è rimasto acceso a lungo; cfr. sezione *Il pacchetto cron* a pagina 144.

RUN_UPDATEDB="no"
La banca dati per locate (`locate`) va aggiornata una volta al giorno. Per una configurazione dettagliata del programma updatedb impostate le seguenti variabili (cfr. i commenti).

RUN_UPDATEDB_AS="nobody"
L'utente sotto la cui identità deve venire eseguito updatedb. L'impostazione di default è qui per motivi di sicurezza `nobody`.

UPDATEDB_NETPATHS=""
updatedb scorre da sè solo directory locali. Potete stabilire comunque le directory di rete da scorrere.

UPDATEDB_PRUNEPATHS="/mnt /cdrom /tmp /usr/tmp /var/tmp /var/spool /proc /media"
Tutte le directory qui riportate vengono ignorate da updatedb durante la sua ricerca.

UPDATEDB_NETUSER=""
Vedi sopra; qui viene stabilito l'utente sotto la cui identità si deve svolgere la ricerca nei percorsi di rete. `nobody` è un esempio.

UPDATEDB_PRUNEFS=""
updatedb è in grado di escludere oltre a determinate directory anche tipi di filesystemt dalla ricerca.

lvm Il Logical Volume Manager.

mail Impostazioni riguardo l'e-mail.

FROM_HEADER=""
`From:`-Indicare riga per tutto il sistema. Se "", viene utilizzato FQDN; cfr. *Sistema nome di dominio* a pagina 211.

MAIL_CREATE_CONFIG="yes"
SuSEconfig genera un `/etc/sendmail.cf` dalle indicazioni che immettete in `sendmail`. Se preferite la configurazione manuale, impostate questa variabile su `no`.

NULLCLIENT=""
Il "Nullclient" è una macchina che sa inviare esclusivamente delle e-mail. Non riceve e-mail dalla rete e non consegna e-mail localmente. Così il "Nullclient" utilizza POP o NFS per accedere alla casella delle e-mail.

SMTPD_LISTEN_REMOTE="no"
Viene impostato `yes` quando si vogliono accettare e-mail dall'esterno. Per un e-mail server questa impostazione è un "must".

mouse Impostazioni del mouse.

MOUSE=""
L'interfaccia del mouse (per esempio `/dev/ttyS0`). YaST2 o SuSEconfig creano un link da `/dev/mouse` al dispositivo indicato.

GPM_PROTOCOL=""
Il protocollo GPM per il dispositivo registrato in ⟨*MOUSE*⟩. Questo valore viene impostato da YaST2.

GPM_PARAM=" -t $GPM_PROTOCOL -m $MOUSE"
I parametri standard per gpm.

network Directory per la configurazione della rete.

network/config Impostazione generali per la configurazione di rete.

DEFAULT_BROADCAST="+"
Viene analizzata ⟨*DEFAULT_BROADCAST*⟩ se non vi è altra indicazione `BROADCAST`. Potete scegliere tra `""` per nessun indirizzo Broadcast, `-` per ⟨*IPADDR*⟩ senza host bits e `+` per l'indicazione completa di ⟨*IPADDR*⟩ con tutti gli host bits.

CHECK_FOR_MASTER="yes"
Questa registrazione fa in modo che l'interfaccia "Master" sia già attivata prima che indirizzi alias, detti anche ("labelled address"), possano essere impostati. Da un punto di vista tecnico questa registrazione non ha alcuna effetto, ma ne traggono un vantaggio gli utenti di ifconfig.

CHECK_DUPLICATE_IP="yes"
Se impostata su `yes`, lo script ifup controlla se un indirizzo Ip viene già utilizzato. Assicuratevi che il kernel supporti sockets di pacchetti (⟨*CONFIG_PACKET*⟩), per garantire la funzionalità ARP dalla quale dipende questo feature. Il controllo dura un secondo per interfaccia, che si fanno sentire nel caso di un notevole numero di indirizzi IP

DEBUG="no"
Abilitare/disabilitare messaggi di debug per gli script di rete. Anche se avete scelto l'impostazione `no`, l'opzione `-o debug` vi permette di abilitare i messaggi di debug di singoli script.

USE_SYSLOG="yes"
I messaggi di errore degli script di configurazione devono essere scritti in `syslog`?

MODIFY_RESOLV_CONF_DYNAMICALLY="yes"
Alcuni servizi come `ppp`, `ippp`, `dhcp-client`, `pcmcia` e `hotplug` modificano `/etc/resolv.conf` in determinati orari. Il valore di default è `yes`.

MODIFY_NAMED_CONF_DYNAMICALLY="no"
Vedi ⟨*MODIFY_RESOLV_CONF_DYNAMICALLY*⟩. Se siete insucuri, lasciate il valore di default `no`.

network/dhcp Impostazioni relativia al DHCP (ingl. *Dynamic Host Configuration Protocol*).

Nota

Per configurare una o più interfacce attraverso il DHCP , ⟨*BOOTPROTO*⟩ in `/etc/sysconfig/network/ifcfg-<interface>` deve assumere il valore `dhcp`. Eventualmente a ⟨*STARTMODE*⟩ si deve assegnare il valore `onboot`.

Nota

La maggior parte di queste opzioni viene utilizzata solo da dhcpcd; ISC dhclient utilizza un file di configurazione proprio. Alcune opzioni vengono sovrascritte dalle impostazioni nei file `ifcfg-*`.

DHCLIENT_BIN=""
Quale client DHCP utilizzare? `dhcpcd` per il demone client DCHP oppure `dhclient` per il dhclient ISC? Se non vi è una registrazione, si ha dapprima il tentativo di lanciare dhcpcd. Se ciò non riesce, si tenta con dhclient.

DHCLIENT_DEBUG="no"
Il client DHCP deve essere lanciato nel modo debug? I file log per DHCP Client Daemon si trovano sotto `/var/log/messagesfordhcpcd`, per ISC dhclient sotto `/var/log/dhclient-script`.

DHCLIENT_SET_HOSTNAME="no"
L'hostname deve essere stabilito dal client DHCP? Con `yes` dovete assicurarvi che non vi troviate proprio in una sessione X in corso, quando viene settato l'hostname, altrimenti la vostra variabile ⟨*DISPLAY*⟩ non può essere analizzata correttamente e non potete aprire altre finestre.

DHCLIENT_MODIFY_RESOLV_CONF="yes"
Il client DHCP potrà modificare il vostro `/etc/resolv.conf`? L'impostazione di default è `yes`. Se scegliete `no` o se ⟨*MODIFY_RESOLV_CONF_DYNAMICALLY*⟩ in `/etc/sysconfig/network/config` ha il valore `no`, il file `/etc/resolv.conf` non viene toccato.

DHCLIENT_SET_DEFAULT_ROUTE="yes"
Il gateway di default deve essere determinato dal client DHCP? Se sono in esecuzione diversi processi dhcpcd dovrebbe avere il permesso di farlo solo uno di questi.

DHCLIENT_MODIFY_NTP_CONF="no"
Il client DHCP potrà modificare la configurazione del NTP (`/etc/ntp.conf`)?

DHCLIENT_MODIFY_NIS_CONF="no"
Il client DHCP potrà modificare la configurazione del (`/etc/yp.conf`)?

DHCLIENT_SET_DOMAINNAME="yes"
Sarà il vostro client DHCP a stabilire il nome di dominio del NIS? (Possibile solo se il server offre l'opzione `nis-domain`.)

DHCLIENT_KEEP_SEARCHLIST="no"
Il client DHCP quando scrive un nuovo `/etc/resolv.conf` dovrà utilizzare l'elenco di ricerca di domini già esistente e aggiungerlo a quello che riceve dal server DHCP?

DHCLIENT_LEASE_TIME=""
Qui potete stabilire la durata (in secondi) per la quale il server DHCP cede al client un IP dinamico ("least").

DHCLIENT_TIMEOUT="999999"
Qui potete impostare il "timeout" dopo il quale il client si interrompe automaticamente se non riceve una risposta dal server. Questa impostazione si riferisce solo a dhcpcd.

DHCLIENT_REBOOT_TIMEOUT=""
Questa opzione stabilisce per quanto tempo dhcpcd tenterà di ricevere nuovamente un "lease" precedente (nello stato init reboot), prima di usare un nuovo "lease".

DHCLIENT_HOSTNAME_OPTION="AUTO"
Potete stabilire un determinato hostname che dhcpcd utilizzerà per messaggi DHCP. Il valore di default `AUTO` fa sì che l'hostname venga inviato automaticamente.

DHCLIENT_CLIENT_ID=""
Qui stabile l'ID del cliente da inviare. Se non immettete alcuna registrazione viene inviata l'indirizzo hardware della schede di rete.

DHCLIENT_VENDOR_CLASS_ID=""
Stalibisce il "Vendor Class Identifier".

DHCLIENT_RELEASE_BEFORE_QUIT="no"
Il client deve comunicare al server che non necessità più un indirizzo, così da renderlo nuovamente disponibile? Questa opzione supporta solo dhcpcd.

DHCLIENT_SLEEP="0"
Alcune interfaccie necessitano di un determinato lasso di tempo prima di poter essere inizializzate correttamente Potete indicare qui il tempo di latenza in secondi, mentre il client DHCP aspetta l'inizializzazione. Comunque queste impostazioni vanno fatte separatamente per le singolo interfacce.

network/ifcfg-eth0 Configurare la prima scheda di rete. Le successive impostazioni si lasciano realzzare comodamente con YaST2.

STARTMODE=""
Quando viene attivata l'interfaccia? `onboot` indica che l'interfaccia viene lanciata al momento del boot, `manual` che ifup deve essere lanciato manualmente e `hotplug` che l'attivazione avvenga per hotplug o PCMCIA.

BOOTPROTO=""
Scegliete tra la configurazione IP statica o l'assegnazione di indirizzi dinamica con DHCP (`dhcp`).

IPADDR=""
Qui immettete l'indirizzo IP per la prima scheda di rete.

NETMASK=""
Qui immettete la maschera di rete della vostra rete.

BROADCAST=""
Indicate l'indirizzo broadcast per la vostra rete

PREFIXLEN=""
Immettete la lunghezza del prefisso.

NETWORK=""
L'indirizzo della vostra rete.

network/ifcfg-lo Configurare il dispositivo loopback.

network/wireless La configurazione per wireless LAN. Siete pregati di utilizzare YaST2 ai fini della configurazione.

news Impostazioni per accedere al server NNTP.

ORGANIZATION=""
Il testo qui digitato apparirà in ogni news-posting inviato dall'host interessato. Esempio:
`Archimede, Paperopoli`

NNTPSERVER="news"
L'indirizzo del news-server; se le vostre news arrivano per UUCP e vengono memorizzate localmente, impostate `localhost`.

nfs Il server NFS. I daemon rpc.nfsd rpc.mountd vengono avviati contemporaneamente. Per una descrizione più dettagliata di un server NFS (ad esempio, per sapere di più sulla configurazione delle directory da esportare), vi preghiamo di leggere la sezione *NFS – filesystem ripartiti* a pagina 245.

REEXPORT_NFS="no"
Impostate le variabili su `yes`, per ri-esportare directory NFS o volumi NetWare montati.

onlineupdate Impostazioni per l'update online di YaST2.

YAST2_LOADFTPSERVER="yes"
All'avvio di YOU ("YaST2-Online-Update"), viene aggiornata la lista di server FTP, con wget di `http://www.suse.de`. Questa lista viene inserita su `/etc/suseservers`. Questa variabile va impostata su `no`, se non desiderate aggiornanta la lista.

PROXY_USER=""
L'utente del proxy utilizzato.

PROXY_PASSWORD=""
La password per il proxy utilizzato.

pcmcia Schede PC/sistema PCMCIA.

PCMCIA_SYSTEM="kernel"
Selezionate uno dei due sistemi PCMCIA: `external` o `kernel`. Se è installato solo uno dei due sistemi, il contenuto della variabile viene ignorato.

PCMCIA_PCIC=""
Serve stabilire il driver del socket (chip set); valori validi sono `i82365` o `tcic`, se si usa il sistema PCMCIA "esterno" (cfr. ⟨*PCMCIA_SYSTEM*⟩) e `yenta_socket`, `i82365` o `tcic` con il sistema

PCMCIA `kernel`. Se la variabile è vuota (""), lo script tenterà autonomamente di trovare il driver giusto; la variabile va dunque settata solo se l'identificazione automatica fallisce.

PCMCIA_PCIC_OPTS=""
Determinare i parametri del timing per driver del socket. Una descrizione più dettagliata la trovate sotto `man i82365` o `man tcic` e nel PCMCIA-HOWTO (`/usr/share/doc/packages/pcmcia`) sotto "PCIC_OPTS".

PCMCIA_CORE_OPTS=""
Qui stabilite le opzioni "pcmcia_core". Una descrizione la trovate in `/usr/share/doc/packages/pcmcia` sotto "CORE_OPTS". Queste opzioni sono valide per entrambi i tipi di PCMCIA.

postfix La configurazione delle variabili di Postfix. Utilizzate a questo fine il modulo `mail` di YaST2.

postgresql PostgreSQL.

POSTGRES_DATADIR="~postgres/data"
In quale directory deve trovarsi il database PostgreSQL?

POSTGRES_OPTIONS=""
Le opzioni qui specificate vengono passate al "PostgreSQL Master Daemon" durante l'avvio. Per ulteriori dettagli consultate le pagine di manuale su `postmaster` e `postgresql`. Non utilizzate in questo contesto l'opzione `-D datadir`; Lo startup-script imposta questo valore basandosi su ⟨*POSTGRES_DATADIR*⟩.

powermanagement apmd.

APMD_WARN_LEVEL="10"
Volete ricevere un messaggio di allerta non appena la capicità della batteria scendono al di sotto di un certo livello (indicazione in percentuale)? L'impostazione di default è `10`; con `0` deattivate questa e le tre seguenti opzioni. Ulteriori informazioni su apmd le trovate sotto `man 8 apmd` o nel relativo script init `/etc/init.d/apmd`.

APMD_WARN_ALL="no"
Le avvertenze di apmd devono essere inviate a tutti i terminale? Allora scegliete `yes`, altrimenti verranno registrati nel file Syslog. Il default è `no`.

APMD_WARN_STEP="0"
I messaggi di avvertenza si ripetono non appena la capacità massima della batteria decresce di un determinato valore (⟨*APMD_WARN_STEP*⟩). `0` disabilita questa impostazione.

APMD_CHECK_TIME="0"
apmd controlla di default lo stato della batteria, ogni volta che riceve la segnalazione di un event dal BIOS. Se questo controllo deve avvenire più spesso, impostate questa variabile su un valore > di 0 secondi. Questo però comporta che il vostro hard disk viene riattivato ad ogni controllo. Il default è `0`.

APMD_DEBUG="no"
Gli script apmd e apmd_proxy possono essere resi più "verbosi". Con `yes` venite informati quando e come viene inizializzato apmd_proxy. Se volete vedere tutto quanto succede all'interno di apmd_proxy sui canali `stdout` e `stderr`, selezionate `error`. Con `all` non vi sfugge nulla. `no` è il default.

APMD_ADJUST_DISK_PERF="no"
Per ragioni di risparmio energetico dovreste settare l'esecuzione dello shutdown dopo un certo periodo di inattività del vostro disco rigido. Se però avete dei processi in corso che ad intervalli regolari o spesso scrivono sul disco, questa opzione è di poca utilità. Questa opzione è disabilitata di default.

APMD_BATTERY_DISK_TIMEOUT="12"
Stabilite un "timeout" dopo il quale verrà eseguito l'arresto del sistema. Bisogna comunque considerare che il valore di questa variabile non si misura in minuti o secondi. Per avere ulteriori dettagli leggete la pagina di manuale di hdparm. Chiaramente questa impostazione rivela la propria utilità se prima avete impostato ⟨*ADJUST_DISK_PERF*⟩ su `yes`.

APMD_AC_DISK_TIMEOUT="0"
Si deve arrestare il disco rigido anche quando il computer è connesso alla rete elettrica? Nel caso affermativo, quando (vd. sopra)? Questa opzione è disabilitata per default

APMD_BATTERY_LOW_SHUTDOWN="0"
Alcuni Bios di portatili inviano un messaggio "battery low" dopo che la capacità della batteria scende al di sotto di un certo valore. Potrete eseguire lo shutdown del vostro sistema automaticamente dopo un determinato lasso di tempo. Indicate un valore in minuti. `1` è il valore minimo, `0` disabilita questa funzione.

APMD_SET_CLOCK_ON_RESUME="no"
Se dopo un standby o suspend sorgono delle difficoltà dovute alle vostre impostazioni di tempo, impostate questa variabile su `yes`. Così il kernel time (orario del kernel) viene impostato automaticamente sul valore della variabile GMT. Questa opzione è disabilitata per default.

APMD_SUSPEND_ON_AC="yes"
Il vostro sistema si arresta anche se connesso alla rete di corrente. Con no disabilitate questa funzione.

APMD_PCMCIA_SUSPEND_ON_SUSPEND="no"
Se la vostra scheda PCMCIA non offre il supporto APM, incaricate apmd di portare la vostra scheda nel modo suspend prima del suspend dell'intero sisteam.

APMD_PCMCIA_EJECT_ON_SUSPEND="no"
Alcune schede PCMCIA (soprattutto schede SCCSI) non reagiscono in modo appropriato al suspend. Per tale ragione potrebbe rilevarsi necessario di disabilitarle con `cardctl eject`.

APMD_INTERFACES_TO_STOP=""
Se la configurazione della vostra scheda di rete integrata non funziona bene con il ciclo suspend/resume, impostate qui il nome dell'interfaccia. L'interfaccia indicata verrà arrestata e riavviata correttamente ad ogni ciclo di suspend/resume.

APMD_INTERFACES_TO_UNLOAD=""
Se la vostra interfaccia di rete non si dovesse arrestare correttamente dopo aver analizzato ⟨*APMD_INTERFACES_TO_STOP*⟩, immettete qui il modulo driver della vostra interfaccia di rete che al suspend verrà caricato dalla memoria e al resume verrà riletto dalla memoria.

APMD_LEAVE_X_BEFORE_SUSPEND="no"
Con alcune schede grafiche la ripresa del modo grafico non funziona correttamente dopo un suspend. Prima del suspend avete la possibiltà di andare sulla console di testo e dopo il resume di ritornare sulla X console. Default è `0`.

APMD_LEAVE_X_BEFORE_STANDBY="no"
Vedi ⟨*APMD_LEAVE_X_BEFORE_SUSPEND*⟩. A volte necessario anche con un standby. Default: `0`.

APMD_LOCK_X_ON_SUSPEND="no"
apmd deve "bloccare" il vostro display? Se nel vostro sistama gira solo un X server, e nessuno ha accesso al vostro sistema attraverso un terminale virtuale, questo è uno stato che si potrebbe definire "sicuro". Una partizione cifrata per i vostri dati offre ulteriore sicurezza, nel caso di furto del vostro laptop. Default: `0`.

APMD_STOP_SOUND_BEFORE_SUSPEND="no"
Il ciclo di suspend/resume a volte causa dei problemi coi moduli suono. Qui potete immettere i moduli da eliminare dalle memoria prima di un suspend ed da ricaricare al resume. Prima di un suspend dovete

spegnere tutte le applicazioni audio. A secondo del sound system assegnate a questa variabili il valore `alsa`, `oss` o `kernel`. Con `no` non viene eseguito alcun "unload" dei moduli sonori.

APMD_KBD_RATE=""
Eventualmente va reimpostata la velocità di ripetizione dei tasti e la velocità di reazione. Immettete un valore numerico possibile o lasciate vuote le variabili se non desiderate delle modifiche.

APMD_KBD_DELAY=""

APMD_TURN_OFF_IDEDMA_BEFORE_SUSPEND=""
Alcuni notebook non ritornano correttamente nella normale modalità di funzionamento se il disco rigido è entrato nel modo DMA. Immettete qui tutti i dischi che necessitano lo spegnimento del modo DMA per ritornare nella modalità di funzionamente normale.

printer Stampante.

DEFAULT_PRINTER="lp"
Il nome della stampante standard, se al comando `lpr` non viene indicato alcuna stampante con `-P`.

proxy Impostazioni del proxy.

HTTP_PROXY=""
Alcuni programmi (ad esempio, lynx, arena o wget) possono usare dei proxy server, se questa variabile ambientale è impostata di conseguenza; SuSEconfig può inserirla su `/etc/SuSEconfig/*` (cfr. nella banca dati di supporto, `file:/usr/share/doc/sdb/en/html/lynx_proxy.html`). Esempio:
`"http://proxy.provider.de:3128/"` .

FTP_PROXY=""
Proxy per FTP. Esempio: `"http://proxy.provider.de:3128/"` .

NO_PROXY="localhost"
Con questa variabile si possono escludere (sotto)domini dal proxy. Esempio: `"www.me.de, do.main, localhost"` .

security Impostazioni della sicurezza di sistema.

CHECK_PERMISSIONS="set"
Determina se i diritti del file debbano essere controllati dai valori del file `/etc/permissions`. Con `set` vengono corrette impostazioni errate, con `warn`, vengono emessi solo degli "Avvertimenti", mentre `no` disattiva questa funzione.

PERMISSION_SECURITY="easy local"
Con `/etc/permissions.paranoid`, `/etc/permissions.secure` e `/etc/permissions.easy` abbiamo tre livelli di sicurezza. Immettete `easy`, `secure` o `paranoid`; alcune impostazioni possono essere eseguite per esempio in `/etc/permissions.local` e poi aggiungere l'estensione `local` come valore .

Considerate che selezionare l'opzione `paranoid` potrebbe limitare l'uso di alcuni servizi di sistema, il che vuol dire che dovrete andare ad attivare questi servizi uno per uno, se ne avete bisogno!

Attenzione: Quando eseguite i valori di `/etc/permissions.local`, controllate che essi non siano in conflitto con quelli del meccanismo di rotazione (pacchetto `logrotate`). logrotate sovrascrive i valori di `/etc/permissions.local`; cfr. sezione *File di log – il pacchetto logrotate* a pagina 144.

sendmail Le variabili di sendmail; utilizzate il modulo `mail` di YaST2 ai fini della configurazione.

sound Informazioni sulla configurazione dell'audio

LOAD_SEQUENCER="yes"
I ALSA Sequencer Module devono essere caricati al boot-up? Queste module vi servono solo se lavorate con dispositivi MIDI. Altrimenti deattivate questa opzione. I moduli possono essere caricate automaticamente in un secondo momento.

ssh Il "Secure Shell Daemon"; prima di avviarlo, assicuratevi di avere una una "host key" – cfr. la documentazione sotto unter `/usr/share/doc/packages/ssh` e le pagine di manuale.

SSHD_OPTS=""

suseconfig Impostazioni di base di SuSEconfig.

ENABLE_SUSECONFIG="yes"
Stabilisce se SuSEconfig debba eseguire la configurazione. Non disattivate assolutamente questa funzione, se volete usufruire del nostro supporto all'installazione.

MAIL_REPORTS_TO="root"
Stabilire a chi SuSEconfig debba inviare via posta elettronica i rapporti compilati durante l'amministrazione del sistema automatica.

MAIL_LEVEL="warn"
Qui, sono possibili due livelli: `warn` spedisce solo le comunicazioni importanti, mentre `all` spedisce anche i file di protocollo ("log files").

CREATE_INFO_DIR="yes"
Determina se il file `/usr/share/info/dir` che rappresenta un indice di tutte le pagine di informazione disponibili debba essere compilato automaticamente con uno script Perl.

CHECK_ETC_HOSTS="yes"
Stabilisce se SuSEconfig debba controllare ed eventualmente modificare il `/etc/hosts`.

BEAUTIFY_ETC_HOSTS="no"
Se desiderate ordinare `/etc/hosts`.

SORT_PASSWD_BY_UID="no"
Ordinare `/etc/passwd` e `/etc/group` secondo "UID" o "GID".

CWD_IN_ROOT_PATH="no"
Directory attuale (ingl. *current working directory*) nel percorso dell'utenteroot; si sconsiglia per motivi di sicurezza. Questa impostazione riguarda tutti gli utenti con un UID inferiore a 100 (ingl. *system user*).

CWD_IN_USER_PATH="yes"
La directory attuale (ingl. *current working directory*) deve risiedere nel percorso dell'utente normale?

CREATE_PERLLOCAL_POD="yes"
`yes` permette a SuSEconfig, di modificare il file `perllocal.pod`. In `perllocal.pod` sono contenute le specifiche di installazione di singoli moduli Perl.

UPDATE_GROFF_CONF="yes"
Aggiornare `DESC` per impostare correttamente le dimensioni della pagina.

GROFF_PAGESIZE=""
Se le dimensioni della pagina non sono evincibili da `/etc/printcap`, impostatele qui. I valori `letter`, `legal`, `a4` e `a5` sono supportati da groff e ghostscript.

sysctl Controllare il sistema al livello del kernel.

IP_DYNIP="no"
Attivare la patch IP dinamica al boot. Con il valore `yes`, lo script `/etc/init.d/boot.proc` attiva questa patch tramite una registrazione nel file system `/proc`.

IP_TCP_SYNCOOKIES="yes"
Attivare la protezione dal "Syn Flooding" (ingl. *syn flood protection*); cfr. `/usr/src/linux/Documentation/Configure.help`.

IP_FORWARD="no"
Se il PC si deve servire di due interfacce di rete, impostate IP_FORWARD su `yes`; questo è il caso con un "router".

ENABLE_SYSRQ="no"
Per visualizzare l'interno del kernel. Prima di utilizzare questa opzione, leggere `/usr/src/linux/Documentation/sysrq.txt`!

DISABLE_ECN="yes"
`yes` disattiva l'ECN (ingl. *early congestion notification*) al momento del boot; utile in caso di difficoltà di connessione con altri host su Internet, i quali per motivi di configurazione del firewall rifiutino i pacchetti di rete, nonostante la connessione abbia funzionato con il kernel 2.2.

BOOT_SPLASH="yes"
Disattivare lo "Splashscreen" al momento del boot.

syslog Configurare il demone syslog.

KERNEL_LOGLEVEL="/var/lib/dhcp/dev/log"
Registrazione aggiuntiva generata dal pacchetto `dhcp-server`. Immettendo il comando `-a <NOMEFILE>`, il nome del file qui registato viene aggiunto automaticamente come socket aggiuntivo attraverso ⟨*SYSLOGD_PARAMS*⟩, non appena viene lanciato syslogd. Il socket aggiuntivo è necessario affiché ad un dhcpd "chrooted" possa continuare con il logging dopo un riavvio di syslogd.

KERNEL_LOGLEVEL="1"
Loglevel per klogd.

SYSLOGD_PARAMS=""
Parametro per syslogd; per esempio `"-r -s my.dom.ain"`.

syslog-ng Configurare Syslog-ng.

SYSLOG_NG_REPLACE="yes"
syslog-ng dovrà sostituire il "vecchio" syslogd? Se questa variabile viene impostata su `no`, vengono lanciati entrambi i programmi.

SYSLOG_NG_PARAMS=""
Consegna dei parametri a syslog-ng. Per ulteriori dettagli consultate `man 8 syslog-ng`.

tetex TEX/LATEX.

CLEAR_TEXMF_FONTS="no"
Per quanto riguarda la creazione automatica dei font per il sistema TeX/LaTex, i font bitmap vengono depositati nella directory `/var/`

cache/fonts/. Se impostate questa variabile su yes, i font che si trovano in queste directory e che non sono stati utilizzati per un periodo oltre a 20 giorni vengono cancellati ad intervalli regolari.

windowmanager Windowmanager.

DEFAULT_WM="kde"
Impostazioni possibili: kde, gnome, fvwm etc.

INSTALL_DESKTOP_EXTENSIONS="yes"
Installare estensioni di SuSE per nuovi utenti. In questo caso, si parla anche di "themes" e funzioni supplementari che rendono il sistema più semplice da usare.

KDE_USE_FAM="no"
Il demone fam; utile solo in concomitanza con directory montate via NFS.

KDE_USE_FAST_MALLOC="yes"
Usare la versione migliorata di malloc.

SUSEWM_UPDATE="yes"
Determina se SuSEconfig debba adeguare i file di configurazione del sistema per il window manager secondo i pacchetti software installati.

SUSEWM_WM="all"
Elenco dei window manager, per i quali creare file di configurazione; valori possibili: fvwm, fvwm2, fvwm95, bowman, mwm, ctwm, kwm sowie all (per tutti).

SUSEWM_XPM="yes"
pacchetto 3dpixms deve essere installato, affinché in fvwm/fvwm95 appaiano i pixmaps nei menu; se questo rallenta il window manager, impostare la variabile su no.

xdmsc Per l'uso di terminali X.

START_RX="no"
Prima di modificare questa variabile, editare il file /etc/inittab eliminando la riga /sbin/init.d/rx. Inoltre vanno impostate le variabili ⟨*RX_XDMCP*⟩ e ⟨*RX_RHOST*⟩. Poi impostate questa variabile su yes per avere un terminale X.

RX_XDMCP="broadcast"
Configurazione del XDMCP (ingl. *XDM Control Protocol*) Requests. query – chiedere una finestra di login ad un server XDM, indirect – chiedere un chooser-menu ad un server XDM e broadcast – chiedere una finestra di login a tutti i server XDM in rete; vince il primo. Per le opzioni query e indirect deve essere settata ⟨*RX_HOST*⟩.

RX_RHOST=""
Nome del host XDM.

RX_DSP=""
Qui potete (facoltativo) stabilire il numero display. Default: `:0`.

RX_BPP=""
Stabilire la profondità dei colori del X server locale (facoltativo).

RX_CLASS=""

xntp Lancia il "Network Time Protocol (NTP) Daemon" dal pacchetto pacchetto `xntp`; la configurazione avviene attraverso il file `/etc/ntp.conf`.

XNTPD_INITIAL_NTPDATE="AUTO-2"
La lista dei server NTP, ripartita da spazi, dai quali potete vedere l'orario prima che venga inizializzato il server locale; per esempio "`sole.cosmo.com`".

Sussiste anche la possibilità di immettere `AUTO`, allora verranno interrogati tutti i server e peer configurati in `/etc/ntpd.conf`. Inoltre il numero complessivo dei server da interrogare si lascia limitare attraverso l'aggiunta di un numero; Default: `AUTO-2`.

Gli orologi radiotelecomandati hanno degli indirizzi del tipo `127.127.T.U`, laddove `T` stia per il tipo di orologio e `U` per il cosiddetto "unit number", un valore tra `0` e `3`. La maggior parte di questi orologi hanno bisogno di un'interfaccia seriale o un bus speciale. Il file di questi dispositivi (device) viene normalemente indicato da un link simbolico `/dev/device-U` all'hardware vero e proprio; `U` deve essere identico allo "unit number". Cfr. anche `/usr/share/doc/packages/xntp/html/refclock.htm`.

Esempio: Chi ha un tale orologio che sia connesso ad un'interfaccia seriale, ha bisogno anche del relativo Symlink, il cui nome si trova su `refclock.htm`. Tutti gli altri normali ricettori del tipo DCF77 hanno il driver "PARSE":

```
## Type 8 Generic Reference Driver (PARSE)
## Address:     127.127.8.u
## Serial Port: /dev/refclock-u
```

Se selezionate il valore `server 127.127.8.0` con la riga `ntp.conf`, avrete anche bisogno di un Symlink di `/dev/refclock-0` su `ttySx` (laddove `x` è l'interfaccia a cui è collegato l'orologio radiotelecomandato

ypbind Configurazione del client NIS. Ulteriori informazioni: Il nome di dominio si trova direttamente in `/etc/defaultdomain`. Il server vie-

ne registrato direttamente in `/etc/yp.conf` durante la configurazione con YaST2; cfr. sezione *NIS – Network Information Service* a pagina 240.

YPBIND_OPTIONS=""
Opzioni.

YPBIND_LOCAL_ONLY="no"
Impostate l'opzione su `yes`, ypbind si connette solo ad interfacce loopback locali. Altri host non gli potranno inviare interrogazioni.

YPBIND_BROADCAST="no"
Se impostate questa opzione su `yes`, ypbind ignora il file `/etc/yp.conf` e cerca di trovare attraverso una chiamata broadcast un server NIS disponibile nella sottorete locale. Evitate di questa opzione a causa delle falle di sicurezza.

YPBIND_BROKEN_SERVER="no"
Se nella vostra rete vi è un server NIS che si collega solo con porte superiori a 1024, questa opzione va impostata su `yes`. Comunque questo rappresenta un rischio in tema di sicurezza. – Dovreste prendere in considerazione l'utilizzo di un 'altra implementazione di server NIS.

ypserv Impostazioni per la configurazione del server NIS

YPPWD_SRCDIR="/etc"
Qui potete immettere una directory per i file sorgenti per `passwd`, `shadow` e wertgroup.

YPPWD_CHFN="no"
L'utente potrà modificare il suo campo GECOS (con ulteriori informazioni come numeri telefonici etc.) attraverso ypchfn etc.)?

YPPWD_CHSH="no"
L'utente potrà modificare il suo login standard con ypchsh?

zope Configurazione di un sistema ZOPE.

ZOPE_FTP="yes"
Zope dovrà offrire un accesso al FTP?

ZOPE_FTP_PORT="8021"
Attraverso quale porta si dovrà realizzare l'accesso?

ZOPE_HTTP_PORT="8080"
Se Zope dovrà fungere da server Web standalone dovrete stabilire la porta che occuperà.

Parte III

Networking

Fondamenti del collegamento in rete

Linux che è nato grazie all'Internet, offre tutti gli strumenti di rete necessari per l'integrazione in diverse strutture di rete. In questo capitolo, vi presentiamo il protocollo TCP/IP normalmente usato da Linux, con tutti i suoi servizi e le sue proprietà. Vi mostreremo come realizzare con SuSE Linux Enterprise Server e l'aiuto di YaST2 l'accesso alla rete utilizzando una scheda di rete. Parleremo dei file centrali di configurazione e verranno elencati alcuni dei tool più importanti.

Dato che la configurazione di una rete può assumere diversi gradi di complessità, in questo capitolo descriveremo solo i meccanismi di base.

TCP/IP: il protocollo usato da Linux 204
IPv6 – l'Internet di prossima generazione 212
L'integrazione nella rete 218
Configurazione manuale della rete 221
Il routing con SuSE Linux Enterprise Server 228
DNS – Domain Name Service 230
NIS – Network Information Service 240
NFS – filesystem ripartiti 245
DHCP 250

TCP/IP: il protocollo usato da Linux

Linux ed altri sistemi operativi Unix usano il cosiddetto protocollo TCP/IP: non si tratta proprio di un unico protocollo rete, bensì di un insieme di protocolli che offrono servizi differenti. TCP/IP deriva da uno sviluppo di applicazioni militari e, nella forma usata oggi, è stato definito circa nel 1981 in un cosiddetto RFC. RFC (ingl. *Request for comments*) sono documenti che descrivono i diversi protocolli Internet ed il procedimento da seguire durante l'implementazione del sistema operativo e delle applicazioni. Potete accedere direttamente a questi documenti RFC tramite web; l'URL è: `http://www.ietf.org/`. Nel frattempo, il protocollo TCP/IP è stato migliorato, ma il fondamento del protocollo è rimasto invariato dal 1981.

Suggerimento

I documenti RFC spiegano la struttura dei protocolli di Internet. Se volete approfondire le vostre conoscenze su un determinato protocollo, i documenti RFC sono la fonte giusta. `http://www.ietf.org/rfc.html`

Suggerimento

I servizi nominati nella tabella 9.1 a fronte, sono disponibili per scambiare i dati fra due computer Linux usando TCP/IP:

Protocollo	Descrizione
TCP	(ingl. *Transmission control protocol*) Un protocollo sicuro ed orientato al collegamento diretto. Dal punto di vista dell'applicazione, i dati da trasmettere vengono inviati come flusso di dati e convertiti dal sistema operativo stesso nel formato adatto alla trasmissione. I dati arrivano all'applicazione-meta che si trova sul computer-meta allo stesso modo in cui sono stati spediti. TCP assicura che non vadano persi dei dati per strada e che non vengano mescolati. TCP viene usato dove è saliente la sequenza dei dati che rende importante la creazione di un collegamento stabile.

Tabella 9.1: *Continua alla pagina seguente...*

UDP	(ingl. *User Datagram protocol*) Un protocollo sciolto e poco sicuro: i dati vengono spediti in pacchetti e i pacchetti di dati vengono creati dall'applicazione. La sequenza dei dati che giunge al ricevente non è garantita e può succedere che vadano persi dei singoli pacchetti di dati. UDP è adatto per applicazioni orientati al set di dati e ha una latenza inferiore al TCP.
ICMP	(ingl. *Internet control message protocol*) Fondamentalmente, questo non è un protocollo per utenti, ma uno speciale protocollo di controllo, che trasmette comunicazioni di errori ed è in grado di verificare il comportamento dei computer interessati alla trasmissione di dati con TCP/IP. Inoltre, con ICMP, viene messo a disposizione anche uno speciale "modo echo" che può venire esaminato con il programma ping.
IGMP	(ingl. *Internet group management protocol*) Questo protocollo regola il comportamento dei computer che usano il multicast IP. Purtroppo, in questo ambito, non possiamo presentarvi il multicasting IP.

Tabella 9.1: *Diversi protocolli del gruppo di protocolli TCP/IP*

Quasi tutti i protocolli hardware lavorano a pacchetti. I dati da trasmettere vengono riuniti in piccoli "pacchetti" e non possono venire spediti in una volta sola. Per questo, anche TCP/IP lavora con piccoli pacchetti di dati. La grandezza massima di un pacchetto TCP/IP è di appena 64 Kilobyte. Normalmente, in pratica, i pacchetti sono molto più piccoli, poiché l'hardware della rete è un fattore restrittivo: ad esempio, il volume di un pacchetto di dati su Ethernet è limitato a 1500 byte. Conseguentemente, la grandezza del pacchetto TCP/IP viene limitata (se i dati vengono trasmessi tramite Ethernet). Nel caso se ne vogliono trasmettere di più, il sistema operativo deve inviare più pacchetti di dati.

Modelli a strati

Tramite IP (ingl. *Internet protocol*) si ha una trasmissione di dati insicura. TCP (ingl. *Transmission control protocol*) è in un certo senso solo un "sopralzo" dell'IP, che garantisce una trasmissione sicura dei dati. IP a sua volta è anche un sopralzo del protocollo sottostante indipendente dall'hardware, p.e

Ethernet. Così si parla di “modello a strati”. A riguardo, osservate anche la figura 9.1.

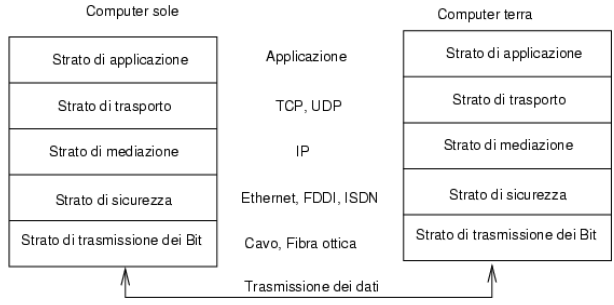


Figura 9.1: *Modello a strati semplificato per TCP/IP*

Nella figura sono menzionati uno o due esempi per il rispettivo strato. Come vedete, gli strati sono disposti secondo il “livello di astrazione”; lo strato inferiore è molto vicino all’hardware. Lo strato superiore invece, esegue un modello quasi completamente astratto dell’hardware sottostante. Ogni strato ha una funzione speciale che si deduce già dal nome. Ad esempio, la rete usata (p.e. Ethernet) viene simboleggiata dallo strato di trasmissione dei bit e dallo strato di sicurezza.

- Mentre lo strato 1 si occupa del tipo di cavi, delle forme dei segnali, della cifratura dei segnali e cose simili, lo strato 2 è responsabile per il procedimento di accesso (quale computer può inviare dati e quando?) e la correzione degli errori (sicurezza dei dati, perciò strato di sicurezza). Lo strato 1 viene nominato strato di trasmissione dei bit.
- Lo strato 3 a sua volta, strato di mediazione è responsabile per la trasmissione di dati su lunghe distanze. Lo strato di mediazione, assicura che i dati arrivino al ricevente giusto.
- Lo strato 4, lo strato di trasporto, si occupa dei dati dell’applicazione: assicura che i dati arrivino a destinazione nella sequenza giusta e che nessuno vada perso. Lo strato di sicurezza controlla solo che i dati che arrivano siano corretti. Lo strato di trasporto evita la “perdita” di dati.
- Lo strato 5 infine, è l’elaborazione dei dati tramite l’applicazione stessa.

Affinché ogni strato possa adempiere ai suoi compiti, devono venire memorizzate altre informazioni nel pacchetto di dati dello strato corrispondente.

Ciò avviene nell'header, l'intestazione del pacchetto di dati. Ognuno degli strati aggiunge, all'inizio del pacchetto in via di formazione, un piccolo blocco di dati, la cosiddetta (ingl. *protocol header*) "testata del protocollo". Se osserviamo un qualsiasi pacchetto di dati TCP/IP in viaggio su un cavo Ethernet, esso si compone come rappresentato nella figura 9.2.

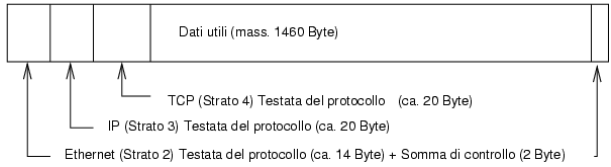


Figura 9.2: *Pacchetto TCP/IP in Ethernet*

Come vedete, il mondo non è ancora perfetto e, soprattutto, privo di eccezioni. La somma di controllo dello stato di sicurezza si trova alla fine del pacchetto e non all'inizio: la cosa, però, è una semplificazione per l'hardware della rete. In un pacchetto, la quantità massima possibile dei dati utilizzabili (per quello che riguarda la rete Ethernet) è di 1460 byte.

Se, perciò, un'applicazione vuole inviare dati tramite la rete, questi attraversano i singoli strati che sono tutti implementati nel kernel di Linux (ad eccezione dello strato 1: la scheda rete). Ognuno degli strati, deve preparare i dati in modo da poterli passare di volta in volta allo strato inferiore. L'ultimo strato, infine, ha il compito di spedire i dati. Al ricevimento dei dati, le cose si svolgono al contrario; da ogni strato, le testate dei protocolli vengono tolte dai dati utilizzabili (proprio come per gli strati di una cipolla). Alla fine, lo strato 4 deve mettere a disposizione di dati per le applicazioni sul computer-meta. Durante questo lavoro, uno strato comunica sempre solo con quello direttamente superiore o inferiore. Per un'applicazione, non fa perciò differenza se i dati vengano trasmessi tramite una rete FDDI di 100 MBit/s o tramite un modem di 56 kbit/s: d'altra parte, per la trasmissione dei dati non è importante quali dati vengano trasmessi, purché siano impacchettati nel modo giusto

Indirizzi IP e routing

Indirizzi IP

Ogni computer nell'Internet riceve un indirizzo inequivocabile di 32 Bit. Normalmente, questi 32 bit o 4 byte vengono scritti come mostrato nella seconda riga della tabella 9.2 nella pagina successiva:

Indirizzo IP (binario):	11000000	10101000	00000000	00010100
Indirizzo IP (decimale):	192.	168.	0.	20

Tabella 9.2: *Sintassi dell'indirizzo IP*

Ogni Byte viene cioè scritto in un sistema di numeri decimali separati l'uno dall'altro da un punto e scritti uno vicino all'altro. L'indirizzo IP è assegnato ad un computer o ad un'interfaccia della rete, e non può quindi venire assegnato nuovamente. Ci sono eccezioni alla regola, ma nelle seguenti considerazioni, non hanno alcuna importanza.

Anche la scheda Ethernet possiede un proprio indirizzo: si tratta del cosiddetto MAC (ingl. *Media access control*), un indirizzo di 48 Bit, univoco in tutto il mondo e memorizzato permanentemente dal produttore della scheda rete nell'hardware del PC. Lo svantaggio di questo indirizzo fisso di fabbrica consiste nel fatto che gli indirizzi MAC non formino un sistema gerarchico, ma siano distribuiti più o meno casualmente e quindi inutili per contattare un host remoto. L'indirizzo MAC occupa però un ruolo molto importante nella comunicazione tra gli host in una rete locale (ed è parte principale della testata di protocollo dello strato 2).

Ed ora ritorniamo agli indirizzi IP: i punti ci indicano già che gli indirizzi IP formano un sistema gerarchico. Fino alla metà degli anni 90, questi indirizzi erano suddivisi in classi: Questo sistema si dimostrò troppo inflessibile e questa suddivisione venne abbandonata. Ora si usa il "routing libero".

Maschere di rete e routing

Poiché, in un primo tempo, il computer con l'indirizzo IP `192.168.0.20` non può sapere dove si trova il computer con l'indirizzo `192.168.0.1`, si escogitò la maschera rete.

Detto in parole povere, in un computer con indirizzo IP, la (sotto)maschera rete definisce che cosa si trova "dentro" e cosa si trova "fuori". I computer che si trovano "dentro" (i professionisti dicono: "nella stessa sottorete"), possono venire interrogati direttamente; quelli "fuori" ("che non sono nella stessa sottorete"), devono venire interrogati tramite un gateway o router. Dato che ogni interfaccia rete può avere un proprio indirizzo IP, avrete intuito che la faccenda può diventare davvero complessa.

Ecco cosa avviene nel computer, prima che possa venire "instradato" un pacchetto rete: l'indirizzo destinatario viene collegato bit dopo bit con la maschera rete AND; successivamente anche l'indirizzo mittente viene collegato

Indirizzo IP:192.168.0.20	11000000	10101000	00000000	00010100
Maschera rete: 255.255.255.0	11111111	11111111	11111111	00000000
Risultato binario	11000000	10101000	00000000	00000000
Risultato decimale	192.	168.	0.	0
Indirizzo IP: 213.95.15.200	11010101	10111111	00001111	11001000
Maschera rete: 255.255.255.0	11111111	11111111	11111111	00000000
Risultato binario	11010101	10111111	00001111	00000000
Risultato decimale	213.	95.	15.	0

Tabella 9.3: *Collegamento degli indirizzi IP con la maschera rete*

bit per bit con la maschera rete AND (vd. tabella 9.3). Di regola, se sono disponibili più interfacce rete, vengono controllati tutti i possibili indirizzi di mittente.

I risultati dei collegamenti AND vengono confrontati. Se i risultati sono esattamente concordanti, significa che il computer destinatario (meta) si trova nella stessa sottorete; altrimenti, deve venire interrogato tramite un gateway. Ciò significa che più bit "1" si trovano nella maschera rete, meno computer possono venire interrogati direttamente e solo tramite un gateway. Per chiarire un pò le cose, abbiamo elencato alcuni esempi nella tabella 9.3.

Anche la maschera rete (come già gli indirizzi IP) viene scritta in numeri decimali divisi da punti: e poiché la maschera rete è inoltre un valore di 32 Bit, vengono scritti 4 numeri uno dopo l'altro. L'utente stesso deve configurare quali siano i computer gateway o con quali interfacce rete debbano essere raggiungibili le aree degli indirizzi.

Ecco ancora un esempio: generalmente, tutti i computer collegati allo stesso cavo Ethernet, si trovano *nella stessa sottorete* e sono direttamente raggiungibili. Anche se Ethernet è suddiviso in cosiddetti switch o bridge, questi computer possono venire raggiunti direttamente.

Se volete superare una distanza abbastanza grande, l'Ethernet più economico non è più adatto e sarete costretti ad inoltrare i pacchetti IP su un altro hardware (p.e. FDDI o ISDN): i device in grado di farlo vengono chiamati router o gateway. Naturalmente, un computer Linux può svolgere questo compito; l'opzione relativa viene nominata ip_forwarding.

Se un gateway è configurato, il pacchetto IP viene inviato al gateway adatto che a sua volta cerca di inoltrarlo (sempre sulla base dello stesso schema). Ciò viene ripetuto su ogni altro computer, finchè il pacchetto non ha raggiun-

to la sua destinazione (meta) o la TTL (ingl. *time to live*)(vita) del pacchetto è esaurita.

Tipo di indirizzo	Descrizione
L'indirizzo di base della rete	È l'indirizzo della maschera rete AND, un qualsiasi indirizzo preso dalla rete: cioè ciò che è raffigurato nella tabella 9.3 nella pagina precedente sotto Risultato. Questo indirizzo non può venire assegnato a nessun computer.
L'indirizzo broadcast	Vuol dire: "contatta tutti i computer in questa sottorete". Per crearlo, la maschera rete viene invertita in modo binario e viene collegata con l'indirizzo di base della rete OR. Dal suddetto esempio risulta quindi 192.168.0.255. Naturalmente, anche questo indirizzo non può venire attribuito a nessun computer.
Il local host	L'indirizzo `127.0.0.1` è attribuito permanentemente su ogni computer al cosiddetto "dispositivo loopback". Con questo indirizzo si può creare un collegamento sul proprio computer.

Tabella 9.4: *Indirizzi speciali*

Poiché, però, in tutto il mondo, gli indirizzi IP devono essere biunivoci, non si possono inventare indirizzi qualsiasi. Per poter però creare ugualmente una rete sulla base IP, esistono tre aree di indirizzi da poter usare senza problemi: con esse però non sarà possibile (senza usare qualche trucco) creare un collegamento con il resto dell'Internet; su Internet, infatti, questi indirizzi non vengono inoltrati.

Si tratta delle aree di indirizzi definite in RFC 1597:

Rete, maschera di rete	Area
10.0.0.0, 255.0.0.0	10.x.x.x
172.16.0.0, 255.240.0.0	172.16.x.x - 172.31.x.x
192.168.0.0, 255.255.0.0	192.168.x.x

Tabella 9.5: *Aree indirizzi IP private*

Sistema nome di dominio

DNS

DNS fa in modo che non dobbiate necessariamente ricordarvi gli indirizzi IP: con l'aiuto di DNS, un indirizzo IP può venire assegnato ad uno o più nomi e viceversa un nome può venire trasformato in indirizzo IP. Sotto Linux questa trasformazione viene normalmente eseguita da un software speciale di nome bind. Il computer che esegue questa trasformazione, si chiama server dei nomi. I nomi formano nuovamente un sistema gerarchico, i cui i singoli componenti del nome vengono divisi da punti. La gerarchia del nome, però, è indipendente dalla gerarchia degli indirizzi IP sopra descritta.

Osserviamo un po' un nome completo, per esempio `laurent.suse.de` scritto nel formato `hostname.dominio`. Un nome completo (in gergo "Fully qualified domain name" o FQDN) consiste nel nome del computer e una parte del dominio. La parte del dominio consiste in una parte liberamente scelta (nel nostro esempio: `suse`) ed nel cosiddetto top level domain, TLD.

L'attribuzione dei TLD è un po' intricata. In America vengono p.e. usati TLD formati da 3 lettere, mentre nel resto del mondo vengono sempre usate le denominazioni ISO dei paesi che consistono di due lettere.

Agli albori di Internet (prima del 1990), esisteva a riguardo un file `/etc/hosts` in cui erano memorizzati i nomi di tutti i computer rappresentati nell'Internet. In breve tempo, a causa della quantità sempre crescente di computer collegati ad Internet, la cosa divenne impraticabile. Per questo, venne creata una banca dati in grado di distribuire e memorizzare i nomi dei computer. Questa banca dati (il server dei nomi sopra menzionato) non accumula i dati di tutti i computer su Internet, ma può delegare ad altri server dei nomi le domande a lui inoltrate.

All'apice della gerarchia, si trovano i "root server dei nomi" che amministrano i top-level domain. I server dei nomi root vengono amministrati dal Network Information Center, ovvero NIC. Il server dei nomi root conosce il server dei nomi di volta in volta responsabile per un top level domain. Nel

caso del top-level domain italiano it l'IT-NIC è responsabile per i domini che finiscono con il TLD it. Sulla pagina web http://www.itnic.it troverete ulteriori informazioni riguardanti IT-NIC; sul top level domain NIC troverete informazioni all'indirizzo http://www.internic.net.

Affinché il vostro computer sia in grado di risolvere un nome in un indirizzo IP, deve conoscere almeno un server dei nomi con un indirizzo IP. La configurazione di un server dei può essere comodamente eseguita con YaST2 Se vi collegate con un modem, può succedere che il protocollo usato per il collegamento fornisca l'indirizzo del server dei nomi durante il collegamento stesso.

DNS sa fare di più, oltre a risolvere nomi di computer. Il server dei nomi, per esempio, "sa" anche quale computer accetta le mail per tutto un dominio; si tratta del cosiddetto Mail exchanger, MX. Su SuSE Linux Enterprise Server, la configurazione dell'accesso del server dei nomi è descritta nel capitolo *DNS – Domain Name Service* a pagina 230.

whois

Il protocollo whois è strettamente "imparentato" con DNS. Con l'omonimo programma whois, potrete velocemente scoprire chi è responsabile per un determinato dominio.

IPv6 – l'Internet di prossima generazione

Perché un nuovo protocollo Internet?

Negli ultimi 10 anni, come conseguenza della creazione di WWW (ingl. *World Wide Web*), l'Internet, e con esso i computer che "parlano" il linguaggio TCP/IP, sono aumentati in modo esplosivo; e da quando, nel 1990, Tim Berners-Lee del CERN http://public.web.cern.ch/ ha inventato il www, il numero di Internet host è aumentato da poche migliaia a ca. 100 milioni.

Come sapete, un indirizzo IP è formato "solo" da 32 Bit. Poiché, per motivi di organizzazione, molti indirizzi IP non possono essere utilizzati, ne vanno persi una certa quantità. Ricorderete certamente che l'Internet è suddiviso in sottoreti, cioè parti di rete. Queste sono sempre formate da una potenza di due meno due indirizzi IP utilizzabili. Per esempio, una sottorete consiste in 2, 6, 14, 30, etc. indirizzi IP. Se, per esempio, volete collegare 128 computer ad Internet, avete bisogni di una sottorete della "classe C" con 256 indirizzi

IP, dei quali solo 254 sono utilizzabili. Come avete visto sopra, in una sottorete vengono a mancare 2 degli indirizzi IP e cioè l'indirizzo broadcast e l'indirizzo di base della rete.

La configurazione di un computer nella rete TCP/IP, è relativamente complicata. Come avete visto, dovrete configurare le seguenti cose sul vostro computer: il proprio indirizzo IP, la maschera rete, l'indirizzo gateway (se esistente) ed un server dei nomi. Tutti questi dati dovete conoscerli o averli ricevuti dal vostro provider.

In ogni pacchetto IP, si trova una somma di controllo che deve venire esaminata e calcolata di nuovo ad ogni procedimento routing: per questo motivo, router molto veloci, necessitano di un'ampia capacità di calcolo che li rende un po' cari.

Finora, alcuni servizi vengono realizzati con broadcast (per esempio il protocollo rete di Windows, SMB). Computer non interessati a questo servizio, sono ugualmente costretti ad elaborare i pacchetti per poi ignorarli, il che, in reti molto veloci, può causare senz'altro un problema.

Il successore di IP, IPv6, risolve tutti questi problemi. L'obiettivo principale dei programmatori era quella di ampliare fortemente l'area d'indirizzo e di semplificare e, se possibile, automatizzare la configurazione delle stazioni di lavoro. In seguito, useremo il termine IPv4 o IP se parliamo del protocollo Internet finora usato e diffuso, IPv6 se si tratterà della nuova versione.

IPv6 viene spiegato più dettagliatamente in RFC 1752. IPv6 usa indirizzi di 128 bit, offre quindi molti bilioni di indirizzi IP; sufficienti anche per una generosa distribuzione di indirizzi. Questa enorme quantità di indirizzi IPv6 permette il lusso di ampliare fino a 48 Bit la sottorete più piccola.

Ciò permette di usare, come componente dell'indirizzo, il sopra citato indirizzo MAC. Poiché questo indirizzo è presente solo una volta al mondo e contemporaneamente viene assegnato permanentemente dal produttore di hardware, esso facilita di molto la configurazione del computer. In realtà, perfino i primi 64 bit vengono riuniti in un cosiddetto token EUI-64: si prendono gli ultimi 48 bit dell'indirizzo MAC, e i rimanenti 24 bit contengono informazioni speciali che rappresentano il tipo di token. Questo rende possibile l'assegnazione di un token EUI-64 anche a computer senza indirizzo MAC (collegamenti PPP e ISDN!).

Inoltre, Ipv6 offre anche una novità: normalmente, ad un'interfaccia di rete vengono assegnati più indirizzi IP. Il vantaggio consiste nel fatto che sono disponibili più reti differenti. Con l'aiuto dell'indirizzo MAC e di un prefisso conosciuto, da una di esse può venire formata una rete configurata in modo completamente automatico; in questo modo, senza bisogno di ulteriori lavori

di configurazione, dopo lo start di IPv6 tutti i computer nella rete locale sono direttamente raggiungibili (con un cosiddetto indirizzo link-local).

Ma anche la rimanente configurazione di una stazione di lavoro può avvenire quasi completamente in modo automatico. A questo scopo, esiste un protocollo speciale con il quale le stazioni di lavoro possono ricevere un indirizzo IP da un router.

Per tutti i computer che appoggiano IPv6, è strettamente prescritto il supporto di "Multicast"; con il suo aiuto, è possibile indirizzare in una volta un gruppo di computer, "broadcast" indirizza tutti i computer di una rete e "unicast" uno solo; esistono anche un paio di gruppi multicast come p.e. "tutti i server dei nomi" (ingl. *all nameservers multicast group*), o "tutti i router" (ingl. *all routers multicast group*).

Poiché un cambiamento di tutti i computer su Internet da IPv4 ad IPv6 non è pensabile, esiste un modo di compatibilità; questo modo riproduce gli indirizzi attuali sugli indirizzi IPv6. Contemporaneamente esistono meccanismi come "tunneling" che impaccano i pacchetti IPv6 in pacchetti IPv4 e li spediscono. Naturalmente sono possibili anche trasformazioni da IPv6 a IPv4 e viceversa. Per poter raggiungere un computer IPv6 da un computer IPv4 è necessario che il computer IPv6 possieda un indirizzo compatibile IPv4.

Configurazione di un indirizzo Ipv6

Potete sicuramente immaginarvi che un indirizzo IPv6, a causa dei 128 bit, è molto più lungo di un indirizzo IPv4 con i suoi 32 bit; l'indirizzo IPv6 ha pur sempre una lunghezza di 16 byte.

A causa della loro dimensione, i nuovi indirizzi IPv6 vengono scritti diversamente dagli indirizzi IPv4. Osserviamo un po' gli esempi nella tabella 9.6 a fronte.

Come potete vedere dalla tabella, gli indirizzi IPv6 vengono raffigurati con numeri esadecimali. I numeri esadecimali vengono sempre raffigurati uniti in gruppi di 2 byte e separati da :. In un indirizzo esistono perciò al massimo 8 gruppi e sette punti doppi. In un gruppo, gli zero-byte di guida possono venire omessi, ma non al centro o alla fine di un gruppo. Più di 4 zero-byte direttamente uno dopo l'altro, possono venire saltati con il segno di omissione ::. In un indirizzo però, è permesso solo un segno di omissione, questo segno non può cioè venire utilizzato più volte. Questo procedimento di omissione, viene chiamato "collapsing". Una raffigurazione speciale sono gli indirizzi di compatibilità IPv4; qui, l'indirizzo IPv4 viene semplicemente "attaccato" al prefisso stabilito per gli indirizzi di compatibilità IPv4.

Descrizione	Valore dell'indirizzo
Localhost	::1
Indirizzi IPv6 compatibili	::10.10.11.102 (IPv6 è supportato)
Indirizzo IPv6 mappato IPv4	::ffff:10.10.11.102 (IPv6 non viene supportato)
Indirizzo qualsiasi	3ffe:400:10:100:200:c0ff:fed0:a4c3
Indirizzo link-local	fe80::10:1000:1a4
Indirizzo site-local	fec0:1:1:0:210:10ff:fe00:1a4
Gruppo multicast "tutti i router link-local"	ff02:0:0:0:0:0:0:2

Tabella 9.6: *Raffigurazione di diversi indirizzi IPv6*

Ogni parte di un indirizzo IPv6 ha un significato definito. I primi byte formano un prefisso ed indicano il tipo di indirizzo. La parte centrale indirizza una rete o non ha alcun significato e la fine dell'indirizzo viene formata dalla parte host.

La tabella 9.7 nella pagina successiva mostra il significato di alcuni prefissi più comuni.

Prefisso (esadecimale)	Uso
00	IPv4 ed IPv4 sugli indirizzi di compatibilità IPv6. Si tratta di un indirizzo compatibile con IPv4. Un router adatto, deve ancora trasformare il pacchetto IPv6 in IPv4. Anche altri indirizzi speciali (p.e.dispositivi loopback) sono muniti di questo prefisso.
Prima cifra 2 o 3	(ingl. *provider-based-unicast*) indirizzi unicast provider-based. Come già successo finora, anche con IPv6 vi possono venire assegnate dal provider parti di rete.
fe80 fino febf	indirizzi (ingl. *link-local*)con questo prefisso non devono venire instradati (routed) e possono perciò venire raggiunti solo nella stessa sottorete.

Tabella 9.7: *Continua alla pagina seguente...*

fec0 fino a feff	(ingl. *site-local*), questi indirizzi possono venire instradati (routed), ma solo entro un'organizzazione. In questo modo, questi indirizzi corrispondono a quelle che finora erano le reti "private" (p.e. 10.x.x.x).
ff	(ingl. *multicast*) indirizzi IPv6 che iniziano con ff, sono indirizzi multicast.

Tabella 9.7: *diversi prefissi IPv6*

Come già osservato sopra, specialmente gli indirizzi unicast sono molto lunghi ed è perciò quasi impossibile tenerli a mente. Perciò per IPv6, un server dei nomi funzionante è ancora più importante che per l'IPv4. L'importanza del server dei nomi viene sottolineata dal fatto che vi è uno speciale protocollo di configurazione automatica solo per lui.

Maschere di rete Ipv6

In IPv6, le maschere rete vengono rappresentate in un altro modo. Poiché già da principio viene usato un routing senza classi e una piccola sottorete può accogliere praticamente una grande quantità di computer, la suddivisione delle reti in classi non ha senso. Poiché nella loro raffigurazione, le maschere rete sarebbero molto lunghe, esse vengono scritte in modo molto differente:

fec0:1:1:0:210:10ff:fe00:1a4/64

significa che gli ultimi 64 bit formano la parte host, mentre i 64 bit anteriori formano la parte della rete dell'indirizzo.

Detto in altre parole 64 significa che la maschera viene riempita, partendo da sinistra con 1 bit, dunque vi sono nella maschera di rete 64 1 bit. Come per IPv4, tramite un collegamento AND della maschera rete, viene stabilito se un computer si trovi nella stessa sottorete o in un'altra.

Documentazione e link su IPv6

Chiaramente quanto riassunto finora non è una introduzione completa ad un tema così vasto come IPv6. Per informazioni più approfondite su IPv6, potete consultare le seguenti fonti online e libri:

http://www.bieringer.de/linux/IPv6/ Linux-IPv6-HOWTO e tanti link.

http://www.6bone.de/ come realizzare un collegamento con IPv6 attraverso un tunnel.

http://www.ipv6.org/ Tutto su IPv6.

RFC 1725 L'RFC introduttivo sul tema IPv6.

L'integrazione nella rete

Oggi si può tranquillamente asserire che TCP/IP è diventato il protocollo rete standard tramite il quale tutti i recenti sistemi operativi riescono a comunicare con TCP/IP. Ciò nonostante, Linux supporta anche altri protocolli rete come, p.e., IPX, usato (in passato) da Novel Netware o anche Appletalk utilizzato dai computer Macintosh. In questo ambito, parleremo solo dell'integrazione di un computer Linux in una rete TCP/IP. Se volete integrare schede di rete "esotiche" come Arcnet, Token-Ring o FDDI, trovate ulteriori informazioni nei sorgenti del kernel `/usr/src/linux/Documentation`.

Premesse

Il computer deve avere una scheda rete supportata. Solitamente, la scheda di rete viene riconosciuta già durante l'installazione e il driver adatto viene automaticamente integrato. Potete vedere se la scheda è stata integrata correttamente dall'output del comando `ifstatus eth0`, indica il device di rete eth0.

Se il supporto del kernel per la scheda di rete viene realizzato come modulo (come è standard nel kernel di SuSE), è necessario registrare come 'alias' il nome del modulo in `/etc/modules.conf`. Per la prima scheda Ethernet per esempio in questo modo: `alias eth0 tulip`. Ciò avviene automaticamente, se in linuxrc, durante la prima installazione, viene caricato il supporto dell'unità di disco per la scheda di rete. Successivamente, questo compito può venire svolto con YaST.

Configurazione con YaST2

Potete eseguire la configurazione della scheda di rete in poco tempo con YaST2. Selezionate nel Centro di controllo la voce 'Rete/Basilare' → 'Configurazione della scheda di rete'. Con 'Modifica' potete modificare le impostazioni della scheda di rete.

Se configurate una scheda di rete su sistemi iSeries, YaST2 visualizzerà tutte le schede di rete ethernet virtuali come 'IBM virtual ethernet card'. Fate clic su 'Termina l'installazione' quando avete completato il processo installivo.

Se avete diversi schede ethernet sul vostro sistema, dovete porre la vostra attenzione sul processo di numerazione dei dispositivi. Annotate quali adapter ha il sistema e quanti ne ha. Quando caricate un modulo, tutte i dispositivi di questo tipo di nomi di dispositivo 'ethx' assegnato. Così il primo dispositivo configurato come 'eth0', l'altro dispositivo dello stesso tipo avrà il numero

di dispositvo ‘eth1’, ‘eth2’, etc. Prendete l’esempio di due schede ethernet IBM 79c970 (feature code 2838 utilizza il driver ‘pcnet32’) schede ethernet e due schede ethernet virtuali su un sistema iSeries. Se configurate una delle schede 79c970 della IBM come ‘eth0’ (ciò accadrà automaticamente in questo caso, l’altra scheda diverrà ‘eth1’ all’avvio del sistema. Dovreste configurare ‘eth2’ come la vostra prima scheda di rete ethernet virtuale selezionando il numero di dispositivo corretto. Ovviamente, ciò può verificarsi anche se disponete di due differenti tipi di schede ethernet fisicali. Dovete conoscere la configurazione del vostro sistema e non dimenticare che una volta un modulo viene caricato, tutti i dispositivi di ogni tipo ricevono dei numeri di dispositivo. Quindi utilizzate lo strumento di configurazione della rete per selezionare i numeri corretti, non dovete configurare ogni singola scheda, assicuratevi solo che il numero di dispositivo è stato settato in modo corretto.

Attivate il punto ‘Hardware’, per modificare, con ‘Modifica’, i dati dell’hardware di una scheda rete già configurata: ora arrivate nel menù della configurazione dei dati dell’hardware della scheda rete. Il menu è rappresentato nella figura 9.3.

Normalmente, YaST2 configura già durante l’installazione il driver per la vostra scheda di rete e attiva la scheda rete stessa: per questa ragione, le impostazioni manuali dei parametri dell’hardware sono necessarie solo se usate più di una scheda rete o se l’hardware della rete non viene riconosciuto automaticamente. In questo caso, selezionate il punto ‘Nuovo’ affinchè possa venir scelto un nuovo modulo del driver.

Figura 9.3: *Configurazione dei parametri dell’hardware*

In questo dialogo, potete impostare il tipo della scheda rete e, nel caso di schede ISA, l'interrupt da usare e l'indirizzo IO. Ad alcuni driver di rete potete dare anche speciali parametri come p.e. l'interfaccia da usare, o se p.e. volete utilizzare sulla scheda il collegamento RJ-45 o BNC. A proposito, osservate la documentazione del modulo driver.

Dopo l'inserzione dei parametri dell'hardware, potete configurare gli altri dati dell'interfaccia della rete. Per attivare la scheda rete appena configurata ed assegnarle un indirizzo IP, selezionate il punto 'Interfaccia' nel dialogo 'Configurazione di base della rete'. Selezionate il numero della scheda e cliccate quindi su 'Modifica': apparirà un nuovo dialogo, nel quale potrete scegliere l'indirizzo IP e gli altri dati della rete IP. Se create una rete individuale, potete orientarVi, per l'attribuzione degli indirizzi, al paragrafo 9 a pagina 204 o alla tabella 9.5 a pagina 211. Altrimenti, registrate nei campi previsti, gli indirizzi assegnati dal Vostro amministratore della rete.

Affinché la risoluzione del nome funzioni come descritto nel capitolo 9 a pagina 230, non dimenticate di impostare un name server sotto 'Nome del computer e name server'. Con il punto 'Routing' potete impostare un routing. Per eseguire impostazioni esperte, selezionate il punto 'Configurazione per esperti'.

La configurazione della rete è a questo punto conclusa. YaST2 lancia SuSEconfig immettete le vostre indicazioni nei relativi file (vd. sezione *Configurazione manuale della rete* a fronte). Affinché le impostazioni vengono rese effettive, dovete riconfigurare i programmi interessati, e riavviare i rispettivi demoni immettendo il comando `rcnetwork restart`.

Configurare IPv6

Se volete configurare l'uso di IPv6, normalmente, non dovete effettuare alcuna configurazione sulle workstation. È però necessario caricare il supporto di IPv6; potete farlo con il comando `modprobe ipv6`

Grazie alla filosofia della configurazione automatica di IPv6, viene attribuito alla scheda rete, un indirizzo nella rete "link-local".

Normalmente, su una workstation, non viene amministrata alcuna tabella routing. La workstation chiede ai router presenti nella rete, con l'aiuto del Router advertisment protocol, quali siano il prefisso e i gateway da usare.

Per installare un router IPv6, potete utilizzare il programma radvd da pacchetto `radvd`, serie `n` (Rete). Questo programma comunica alla workstation, il prefisso da usare per gli indirizzi IPv6 e il/i router.

Per poter assegnare facilmente un indirizzo IPv6 ad una workstation, è quindi consigliabile installare e configurare un router con il programma radvd. In questo modo, le workstation ricevono automaticamente gli indirizzi IPv6.

Configurazione manuale della rete

La configurazione manuale della rete dovrebbe sempre essere la seconda scelta. Noi consigliamo di usare YaST2.

Tutte le interfacce di rete vengano avviate con lo script `/sbin/ifup`. Per fermare o controllare un interfaccia vi è `ifdown` e `ifstatus`.

Se siete in possesso solo di una scheda di rete integrata, basta configurare le interfacce tramite i loro nomi. Con `ifup eth0`, `ifstatus eth0` e `ifdown eth0` avviate, controllate e fermate l'interfaccia di rete `eth0`. I file di configurazione utilizzati si trovano sotto `/etc/sysconfig/network/ifcfg-eth0`. `eth0` è in questo caso contemporaneamente il nome dell'interfaccia e il nome per la configurazione della rete.

La configurazione della rete può essere assegnata anche all'indirizzo hardware (indirizzo MAC) di una schede di rete. Per realizzare ciò, si usa un file di configurazione `ifcfg-<indirizzohardwaresenzaiduepunti>`. L'indirizzo hardware va scritto minuscolo, così come emesso da `ip link`; (`ifconfig` utilizza le maiuscole). Se `ifup` trova un file di configurazione adattato all'indirizzo hardware, viene ignorato possibilmente anche un `ifcfg-eth0` esistente.

File di configurazione

Questo paragrafo riassume i file di configurazione di rete e spiega la loro funzione e il formato utilizzato.

`/etc/sysconfig/network/ifcfg-*` Questi file contengono dati specifici per un'interfaccia di rete. Possono essere denominati secondo il nome dell'interfaccia (`ifcfg-eth2`), l'indirizzo hardware di una scheda di rete (`ifcfg-000086386be3`) o secondo la descrizione hardware per una scheda (`ifcfg-usb`). Se volete fare uso di alias di rete, i file corrispondenti sono semplicemente `ifcfg-eth2:1` o `ifcfg-usb:1`. Lo script `ifup` ottiene all'occorrenza oltre al nome di interfaccia anche una precisa descrizione di hardware, e poi cerca i file che meglio si adattano per la configurazione.

I file contengono l'indirizzo IP (BOOTPROTO="static", IPADDR="10.10.11.214") o l'istruzione di utilizzare DHCP (BOOTPROTO="dhcp"). La maschera di rete può già contenere l'indirizzo IP (IPADDR="10.10.11.214/16") o si può indicarlo separatamente (NETMASK="255.255.0.0"). La pagina di manuale di `ifup` (`man ifup`) contiene l'elenco completo delle variabili.

Inoltre, possono essere utilizzate tutte le variabili dai file `dhcp`, `wireless` e `config` nei file `ifcfg-*`, se una impostazione generale debba venire utilizzata solo per un' interfaccia. Con le variabili `POST_UP_SCRIPT` e `PRE_DOWN_SCRIPT` possono essere eseguiti singoli script dopo l'avvio o prima dell'arresto della interfaccia.

`/etc/sysconfig/network/config,dhcp,wireless` Il file `config` contiene impostazioni generali per il comportamento di `ifup`, `ifdown` e `ifstatus`. Le possibilità sono ben commentate. Similmente vi sono dei commenti in `dhcp` e `wireless`, dove trovate le impostazioni generali per DHCP e schede di rete radio. Tutte le variabili da questi file possono essere utilizzate anche in `ifcfg-*`, e chiaramente hanno lì precedenza.

`/etc/hosts`
In questo file (vedi file 28) vengono assegnati gli indirizzi IP al nome del host. Se non vi è un server dei nomi, tutti gli host verso cui si creerà un collegamento IP dovranno essere elencati qui. Per ogni host si immette una riga che consiste dell'indirizzo IP, il nome del host completamente qualificato e il nome dell'host (per esempio, `terra`). L'indirizzo IP deve trovarsi all'inizio della riga e le registrazioni vanno separate con spazi e tabulazioni. I commenti vengono introdotti da '#'.

```
127.0.0.1 localhost
192.168.0.1 sole.cosmo.com sole
192.168.0.20 terra.cosmo.com terra
```

file 28: `/etc/hosts`

`/etc/networks`
Qui vengono convertiti i nomi della rete in indirizzi di rete. Il formato assomiglia a quello del file-`hosts`, qui però i nomi della rete precedono gli indirizzi (vedi file 29).

```
loopback     127.0.0.0
localnet     192.168.0.0
```

file 29: /etc/networks

/etc/host.conf

L'associazione dei nomi, cioè la traduzione di nomi di computer o reti tramite la libreria *resolver* viene guidata da questo file; questo file viene usato solo per programmi che hanno un link con libc4 o libc5; sui programmi glibc attuali, vedi le impostazioni in `/etc/nsswitch.conf`! Ogni parametro deve trovarsi in una propria riga, commenti vengono introdotti da `'#'`. La tabella 9.8 mostra i parametri possibili.

order *hosts*, *bind*	Sequenza nella quale vengono usati i servizi per l'associazione di un nome. Possibili argomenti sono (separati da uno spazio o virgola): *hosts*: Cercare nel file `/etc/hosts` *bind*: Uso di un server dei nomi *nis*: Tramite NIS
multi *on*/*off*	Decide se un computer registrato in `/etc/hosts` possa avere più indirizzi IP.
nospoof *on* alert *on*/*off*	Questi Parametri influenzano lo *spoofing* nel server dei nomi, non hanno però ulteriore influenza sulla configurazione della rete.
trim ⟨*domainname*⟩	Il nome del dominio indicato viene tagliato dal computer prima che questi risolva il nome del computer (sempre che il nome del computer contenga questo nome di dominio). Questa opzione è d'aiuto se nel file `/etc/hosts` esistono solo nomi di dominio locale che però devono anche venire riconosciuti col nome del dominio attaccato.

Tabella 9.8: *Parametri per /etc/host.conf*

Un esempio per `/etc/host.conf` mostra il file 30.

```
  # We have named running
order hosts bind
# Allow multiple addrs
multi on
```

file 30: /etc/host.conf

/etc/nsswitch.conf

Con la GNU C Library 2.0 è arrivato anche il "Name Service Switch" (NSS) ; vedi la pagina di manuale di `nsswitch.conf` (`man 5 nsswitch.conf`), come pure più dettagliatamente *The GNU C Library Reference Manual*, capitolo "System Databases and Name Service Switch"; vd. pacchetto `libcinfo`, serie `doc`.

Nel file `/etc/nsswitch.conf` viene stabilito in quale successione vengono richieste determinate informazioni. Un esempio per `nsswitch.conf` viene mostrato nel file 31. I commenti vengono introdotti da `'#'`. Lì per esempio, la registrazione nella "banca dati" `hosts`, significa che tramite DNS (vedi il pacchetto `named`), viene inviata una richiesta a `/etc/hosts` (`files`).

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
```

file 31: /etc/nsswitch.conf

Le "banche dati" disponibili tramite NSS sono indicate nella tabella 9.9 a fronte; in futuro ci saranno anche `automount`, `bootparams`, `netmasks` e `publickey`.

`aliases`	mail alias, usato da `sendmail`(8); vedi la pagina di manuale `aliases`.
`ethers`	Indirizzi Ethernet.
`group`	Usato da `getgrent`(3) per gruppi di utenti; vedi la pagina di manuale `group`.
`hosts`	Usato da `gethostbyname`(3) e funzioni simili, per gli hostname e indirizzi IP.
`netgroup`	Elenco, nella rete, di host e utenti per regolare i diritti d'accesso ; vedi la pagina di manuale `netgroup`.
`networks`	Nomi e indirizzi della rete usati da `getnetent`(3)
`passwd`	Password degli utenti usate da `getpwent`(3); vedi la pagina di manuale `passwd`.
`protocols`	Protocolli rete usati da `getprotoent`(3); vedi la pagina di manuale `protocols`.
`rpc`	Nomi e indirizzi "Remote Procedure Call" usati da `getrpcbyname`(3) e da simili funzioni.
`services`	Servizi rete usati da `getservent`(3).
`shadow`	Password "shadow" degli utenti usate da `getspnam`(3); vedi la pagina di manuale `shadow`.

Tabella 9.9: *Banche dati disponibili tramite* `/etc/nsswitch.conf`

Le possibilità di configurazione delle "banche dati" NSS, si trovano nella tabella 9.10.

`files`	Accesso diretto su file, per esempio su `/etc/aliases`.
`db`	Accesso tramite una banca dati.
`nis`	vedi sezione 9 a pagina 240.
`nisplus`	
`dns`	Da usare come estensione solo con `hosts` e `networks`.
`compat`	Da usare come estensione solo con `passwd`, `shadow` e `group`
inoltre	con determinati lookup result è possibile provocare reazioni differenti; dettagli a riguardo si trovano nella pagina di manuale `nsswitch.conf`.

Tabella 9.10: *Possibilità di configurazione delle banche dati NSS*

/etc/nscd.conf

Tramite questo file viene configurato l'nscd (ingl. *Name Service Cache Daemon*); vedi le pagine di manuale pernscd e nscd.conf. Contiene le informazioni di passwd, groups e hosts. Il daemon deve essere riavviato di nuovo se p.e. la risoluzione del nome (DNS) viene cambiata tramite modifiche in /etc/resolv.conf; Usate rcnscd restart per riavviarlo.

Attenzione

Se, per esempio, è attivo il caching per passwd, ci vogliono in genere 15 secondi fino a che un utente locale appena creato non venga riconosciuto dal sistema. Iniziando di nuovo nscd, si può ridurre il tempo d'attesa

Attenzione

/etc/resolv.conf

Come già il file /etc/host.conf, anche questo file, per causa della libreria *resolver*, svolge un ruolo di risoluzione di nomi di computer.

Il dominio a cui appartiene l'host viene specificato in questo file (parola chiave search). Anche lo stato dell'indirizzo (parola chiave server dei nomi) da usare. Può venire dato più di un nome di dominio. Al momento della risoluzione di un nome non pienamente qualificato, si tenda di crearne uno allegando le singole registrazioni search. Diversi server dei nomi si possono contraddistinguere immettendo diverse righe ognuna della quale con name server al principio. I commenti sono preceduti da '#'.

Il file 32 indica un esempio per /etc/resolv.conf.

```
# Our domain
search cosmo.com

name server 192.168.0.1
```

file 32: /etc/resolv.conf

Alcuni servizi, come pppd (wvdial), ipppd (isdn), dhcp (dhcpcd e dhclient), pcmcia e hotplug, modificano il file /etc/resolv.conf tramite lo script modify_resolvconf.

Una volta modificato temporaneamente il file `/etc/resolv.conf` con questo script, esso conterrà un commento definito che dichiarerà da che tipo di servizio è stato modificato, dove è memorizzato il file originale, e come possono essere disattivate le modifiche automatiche.

Se `/etc/resolv.conf` è stato modificato più volte, questa concatenazione di modifiche verrà sempre disattivata ordinatamente, anche se le modifiche sono state eseguite in ordine sparso. Cosa che può tranquillamente succedere, nel caso di isdn, pcmcia e hotplug.

Se avete chiuso un servizio in modo non corretto, è possibile ripristinare lo stato iniziale con `modify_resolvconf`. Durante il caricamento, il sistema verifica la permanenza di eventuali versioni modificate di `resolv.conf` (p.e., a causa di un crollo del sistema), per poi ripristinare la versione originale (non modificata) di `resolv.conf`.

YaST2 usa il comando `modify_resolvconf check` per determinare se `resolv.conf` è stato modificato e di conseguenza avvertire l'utente che le modifiche andranno perse dopo il ripristino del file.

Alternativamente, YaST non si serve di `modify_resolvconf`: in questo caso, lasciar modificare il file resolv.conf a YaST o modificarlo manualmente non fa differenza. In entrambi i casi, si tratta di una modifica mirata e duratura, mentre le modifiche dei servizi menzionati è di natura puramente temporanea.

`/etc/HOSTNAME`
: Qui si trova il "nickname" del computer, cioè solo l'hostname senza il nome del dominio. Durante lo start del computer, questo file viene letto da diversi script; il file può contenere solo una riga sulla quale si trova il nome del computer!

GLi script startup

Oltre ai file di configurazione descritti esistono diversi script che durante lo start del computer, inizializzano i programmi di rete. Questi script vengono avviati non appena il sistema passa in uno dei *runlevel multiutente*, (vd. tabella 9.11 nella pagina seguente).

`/etc/init.d/network`	Questo script si occupa della configurazione dell'hardware e del software di rete durante la fase di avvio del sistema.

Tabella 9.11: *Continua alla pagina seguente...*

/etc/init.d/inetd	Lancia l'inetd nel caso che sia impostato in /etc/rc.config; ciò è necessario se per esempio ci si vuole collegare a questo computer dalla rete.
/etc/init.d/portmap	Lancia il portmapper che è necessario per poter usare i server RPC, come per esempio un server NFS.
/etc/init.d/nfsserver	Inizializza il server NFS.
/etc/init.d/sendmail	Controlla il processo sendmail.
/etc/init.d/ypserv	Lancia il server NIS.
/etc/init.d/ypbind	Lancia il client NIS.

Tabella 9.11: *Alcuni startup script dei programmi della rete*

Il routing con SuSE Linux Enterprise Server

La tabella di routing si imposta nei file di configurazione /etc/sysconfig/network/routes e /etc/sysconfig/network/ifroute-* .

Nel file /etc/sysconfig/network/routes possono venire registrati tutti le route statiche che sono necessarie per i diversi compiti di un sistema: route ad un host, route ad un computer tramite un gateway e route ad una rete.

Per tutte le interfacce che necessitano un routing particolare, ciò si lascia definire in un file proprio per ogni interfaccia: /etc/sysconfig/network/ifroute-*. Al posto di '*' inserite il nome dell'interfaccia. Le registrazioni possono assumere il seguente aspetto:

```
DESTINATION           GATEWAY NETMASK   INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION           GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -         INTERFACE [ TYPE ] [ OPTIONS ]
```

Se GATEWAY, NETMASK, PREFIXLEN o INTERFACE non vengono indicati, al loro posto va inserito un '-'. Le registrazioni TYPE e OPTIONS possono anche essere omesse.

- Nella prima colonna si indica la meta di un route: qui può trovarsi l'indirizzo IP del computer o della rete o, con server dei nomi *raggiungibili*, anche il nome completo, qualificato del computer o di una rete.

- La seconda colonna contiene o il gateway di default o un gateway dietro cui sono raggiungibili o un computer o una rete. .
- La terza colonna contiene il netmask per reti o computer dietro un gateway. Per computer dietro un gateway, la maschera è per esempio `255.255.255.255`.
- L'ultima colonna è importante solo per le reti collegate al computer locale (Loopback, Ethernet, ISDN, PPP, ...). Qui si deve specificare il nome del dispositivo.

I seguenti script nella directory `/etc/sysconfig/network/scripts/` vi assistono nella amministrazione delle route:

ifup-route per impostrare una route

ifdown-route per disabilitare uaa route

ifstatus-route per controllare lo stato delle route

DNS – Domain Name Service

DNS (ingl. *Domain Name Service*) è necessario per risolvere in indirizzi IP i nomi di domain e computer; in questo modo viene p.e. assegnato al nome del computer `terra` l'indirizzo IP `192.168.0.20` . Prima di configurare un proprio name server, leggete le informazioni generali riguardanti DNS che si trovano nel capitolo 9 a pagina 211.

Inizializzare il name server BIND

In SuSE Linux, il name server BIND8 – e questo vale anche per la nuova versione BIND9 – è già preconfigurato in modo da poterlo avviare senza problemi dopo l'installazione.

Se siete già in possesso di un collegamento internet funzionante e registrate in `/etc/resolv.conf` 127.0.0.1 come name server per l'host locale, generalmente sarete già in possesso una risoluzione del nome funzionante, senza conoscere il DNS del provider. BIND esegue così la risoluzione del nome tramite il root name server – e avrà bisogno di molto tempo. Per ottenere una risoluzione del nome sicura ed effettiva, si dovrebbe normalmente registrare sempre nel file di configurazione /etc/named.conf, sotto forwarders, il DNS del provider assieme al suo indirizzo IP. Se la cosa funziona, il name server corre come puro name server "Caching-only". Solo dopo avergli "insegnato" le zone proprie, diventa un vero DNS. Un esempio a riguardo si trova nella directory di documentazione `/usr/share/doc/packages/bind8/sample-config`.

Non si dovrebbe però installare alcun dominio ufficiale, finché non lo si è ricevuto dall'istituzione competente – per '.it' si tratta della ITNIC . Anche se siete in possesso di un dominio personale, che però viene amministrato dal provider, è meglio non utilizzarlo. In caso contrario, BIND non è in grado di inoltrare (forward) le richieste per questo dominio e il web server che si trova dal provider non sarebbe più raggiungibile per il proprio dominio. Per avviare il name server, si registra (come root) sulla riga di comando

```
rcnamed start
```

Se sulla destra, in verde appare "done", il `named`, così si chiama il processo del name server, è stato inizializzato con successo. Sul sistema locale, è possibile provare subito la funzionalità del name server; allo scopo usate il programma `nslookup`. Come default server, deve venire indicato il local host con l'indirizzo 127.0.0.1. Se questo non avviene, in `/etc/resolv.conf` si trova probabilmente un name server errato, o questo file non esiste. Per un

primo test, inserite sul prompt di `nslookup`, "localhost" o "127.0.0.1"; questo dovrebbe sempre funzionare. Se invece ricevete una comunicazione di errore ("No response from server" o qualcosa di simile) controllate, con il seguente comando, se il `named` corre.

```
rcnamed status
```

Se il name server non parte o mostra un comportamento errato, nella maggioranza dei casi, ne troverete la causa protocollata in "/var/log/messages".

Una volta ottenuto il collegamento, fate attenzione che BIND8 (allo start) possa controllare il root name server. Se non riesce, poiché il collegamento internet non è stato realizzato, può accadere che non possa venire risolta alcuna richiesta DNS tranne che per zone localmente definite. In questo caso, BIND9 si comporta diversamente, ma necessita di molte più risorse di BIND8.

Per usare il name server del provider come "forwarder", o per usarne uno già corrente nella propria rete, lo si registra (o se ne registrano diversi) nella sezione Opzioni sotto forwarders; cfr. esempio 33.

```
options {
         directory "/var/named";
         forwarders { 10.11.12.13; 10.11.12.14; };
         listen-on { 127.0.0.1; 192.168.0.99; };
         allow-query { 127/8; 192.168.0/24; };
         notify no;
        };
```

file 33: *Opzioni di forwarding in* `named.conf`

Gli indirizzi IP usati nell'esempio sono arbitrari e devono naturalmente venire registrati secondo i propri dati.

Dopo Opzioni, digitate le zone; avrete bisogno anche del "localhost", quindi lo "0.0.127.in-addr.arpa" e "." del "type hint". I file corrispondenti non avranno bisogno di essere modificati, dal momento che funzionano benissimo così come sono.

Non dimenticate di porre un ";" alla fine di ogni riga e di digitare correttamente le parentesi graffe.

Dopo le modifiche del file di configurazione `/etc/named.conf` o dei file delle zone, caricatele su BIND con il comando `rcnamed reload`.

Alternativamente, reinizializzate il name server con il comando `rcnamed restart`. E per chiudere il name server, usate `rcnamed stop`.

Il file di configurazione /etc/named.conf

Tutte le impostazioni del name server BIND8 o BIND9 devono venire eseguite nel file `/etc/named.conf`. I dati stessi delle zone (i nomi dei computer, gli indirizzi IP, etc.) per i domini da amministrare, devono venire archiviati in file separati nella directory `/var/named`. Ma di questo parleremo nel prossimo capitolo.

Il `/etc/named.conf` si suddivide grossolanamente in due aree: una sezione options per le impostazioni generali e le registrazioni zone per i singoli dominio. Inoltre è anche possibile definire un'area logging, come pure registrazioni del tipo acl. Le righe di commento iniziano con il carattere `'#'`, alternativamente è permesso anche `'//'`.

Il 34 vi mostra un esempio di `/etc/named.conf` minimalistico.

```
options {
        directory "/var/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

file 34: *File minimalistico* `/etc/named.conf`

Questo esempio funziona sia per Bind8 che per Bind9 poiché non vengono utilizzate opzioni speciali che possono essere capite solo da una versione. Bind-9.1.1 accetta tutte le configurazioni di Bind8 e, semmai, annota allo start se un'opzione non è implementata. Speciali opzioni di Bind9 non vengono però supportate da Bind8.

Le opzioni di configurazione più importanti nella sezione options

directory /var/named; indica la directory in cui BIND trova i file con i dati delle zone.

forwarders { 10.0.0.1; }; viene usato per indicare uno o più name server (maggiormente quelli del provider) ai quali vengono inoltrate le richieste DNS a cui non è possibile rispondere direttamente.

forward first; fa in modo che le richieste DNS vengano inoltrate ("forwarded"), prima di cercare di risolverle tramite i root name server. Invece di forward first è anche possibile scrivere forward only; in questo caso, tutte le richieste vengono inoltrate e i root name server non vengono più indirizzati. Può essere conveniente nella configurazione del firewall.

listen-on port 53 { 127.0.0.1; 192.168.0.1; }; indica a BIND, su quali interfacce di rete e quale porta stia aspettando le richieste dei client. L'indicazione port 53 può venire omessa, poiché 53 è il port standard. Omettendo completamente questa registrazione, vengono usate come standard tutte le iinterfacce

query-source address * port 53; questa registrazione può essere necessaria, se un firewall blocca le richieste DNS esterne. In questo modo si induce BIND a inviare richieste all'esterno dal port 53 e non dai port più alti > 1024.

allow-query { 127.0.0.1; 192.168.1/24; }; definisce le reti da cui i client possono porre richieste DNS. /24 è un'abbreviazione per la maschera rete, in questo caso 255.255.255.0.

allow-transfer { ! *; }; regola quali computer possano richiedere il trasferimento delle zone; in questo esempio viene completamente impedito da ! *. Senza questa registrazione, il trasferimento delle zone può venire richiesto da qualunque parte.

statistics-interval 0; senza questa registrazione, BIND8 produce ogni ora più righe di messaggi statistici in `/var/log/messages`. L'indicazione 0 fa in modo che questi messaggi vengano completamente omessi; diversamente qui si può indicare il tempo in minuti.

cleaning-interval 720; questa opzione stabilisce il periodo di tempo in cui Bind8 ripulisce il suo cache. Ogni volta, questa attività provoca una registrazione in /var/log/messages. L'indicazione del tempo avviene in minuti: sono preconfigurati 60 minuti.

interface-interval 0; Bind8 ricerca regolarmente nelle interfacce di rete, nuove o non più esistenti interfacce. Se questo valore è impostato su 0, la ricerca non viene effettuata e Bind8 "ascolta" solo sull'interfaccia trovata allo start. Alternativamente si può indicare l'intervallo in minuti. La preconfigurazione è di 60 minuti.

notify no; no procura che non venga avvisato nessun altro name server se vengono apportate modificazioni ai dati delle zone o se il name server viene avviato di nuovo.

La sezione di configurazione Logging

In Bind8 è possibile in diversi modi configurare, come e dove eseguire un protocollo. Normalmente, dovrebbero essere sufficienti le preimpostazioni. L'esempio 35 vi mostra la forma più semplice e reprime completamente il "Logging":

```
logging {
        category default { null; };
};
```

file 35: *Logging viene soppresso*

Impostazione delle zone

```
zone "mio-dominio.it" in {
       type master;
       file "mio-dominio.zone";
       notify no;
};
```

file 36: *La zone del mio-dominio.it*

Dopo zona viene indicato il nome del dominio da amministrare, qui abbiamo preso arbitrariamente ilmio-dominio.it seguito da un in e da un blocco delle rispettive opzioni, posto fra parentesi graffe; cfr. esempio 36. Se si desidera definire una "zona slave", si cambia solo il type su slave e si indica un name server che amministri questa zona come master (può, però, anche essere uno "slave"); cfr. esempio 37 a fronte

```
zone "altri-domini.it" in {
        type slave;
        file "slave/altri-domini.zone";
        masters { 10.0.0.1; };
};
```

file 37: *La zone per altri-domini.it*

Le opzioni:

type master; il master stabilisce che *questa* zona venga amministrata su *questo* name server. Premessa per questa opzione: un file di zone perfetto.

type slave; questa zona viene trasferita da un altro name server. Deve venire usata con masters.

type hint; la zona . del tipo hint viene impiegata per l'indicazione del root name server. Questa definizione di zona può rimanere invariata.

file ilmio-dominio.zona; file slave/altri-domini.zona; questa registrazione indica il file in cui sono registrati i dati delle zone per il dominio. Con uno slave, il file non è necessario, poiché il suo contenuto viene preso da un altro name server. Per distinguere fra master file e slave file, viene indicata per gli slave file la directory `slave`.

masters 10.0.0.1; ; questa impostazione è necessaria solo per zone slave ed indica da quale name server debba venire trasferito il file delle zone.

allow-update { ! *; }; Questa opzione regola l'accesso ai dati delle zone dall'esterno. Se l'accesso fosse indiscriminato, ogni client potrebbe registrarsi nel DNS del tutto autonomamente, cosa che non è auspicabile per motivi di sicurezza. Senza questa opzione, non sono permesse modifiche delle zone. Il comando dato nell'esempio non cambierebbe nulla, dal momento che la definizione ! * proibische, anch'essa, ogni accesso.

Creazione dei file di zona

Si ha bisogno di due tipi di file di zona: uno per attribuire un indirizzo IP al nome di un PC e l'altro per fare l'esatto contrario, cioè per fornire un nome di PC ad un determinato indirizzo IP.

D'importanza fondamentale è il '.' nei file di zona. A nomi di computer senza il punto, viene sempre aggiunta automaticamente la zona. È quindi necessario porre un '.' alla fine di nomi completi, già provvisti di dominio completo, per evitare che il dominio venga ripetuto due volte. Un punto mancante o sbagliato è sicuramente l'errore più comune nella configurazione di name server.

Il primo caso, ce lo mostra il file di zona `mondo.zona`, responsabile per il dominio `mondo.all`; cfr. il file 38

```
1.  $TTL 2D
2.  mondo.all IN SOA      gateway  root.mondo.all.(
3.              2001040901  ; serial
4.              1D          ; refresh
5.              2H          ; retry
6.              1W          ; expiry
7.              2D )        ; minimum
8.
9.              IN NS       gateway
10.             IN MX       10 sole
11.
12. gateway     IN A        192.168.0.1
13.             IN A        192.168.1.1
14. sole       IN A        192.168.0.2
15. luna        IN A        192.168.0.3
16. terra       IN A        192.168.1.2
17. marte       IN A        192.168.1.3
```

file 38: *File* `/var/named/mondo.zone`

Riga 1: $TTL definisce il TTL standard, valido per l'intero contenuto di questo file: due giorni, in questo caso (2D = 2 days). TTL significa "Time to Live", ovvero 'durata di validità'.

Riga 2: Ha inizio qui il SOA control record:

- Al primo posto viene il nome del dominio da amministrare mondo.all, chiuso da un '.', per evitare che venga aggiunta la zona una seconda volta. Alternativamente, si può digitare una chiocciola `'@'`, con la quale la zona viene evinta dalla rispettiva registrazione nel `/etc/named.conf`.

- Dopo l'IN SOA, abbiamo il nome del name server, responsabile di questa zona, in funzione di master. In questo caso, il nome gateway, relativo a gateway.mondo.all viene completato automaticamente, perché non seguito da `'.'`.
- Segue l'indirizzo di e-mail della persona responsabile di questo name server. Dal momento che la chiocciola @ possiede già un significato particolare, si aggiungerà semplicemente un `'.'`, di modo che, per root@mondo.all si avrà root.mondo.all.. Non dimenticate il punto alla fine, altrimenti viene aggiunta la zona un'ennesima volta.
- Alla fine abbiamo una `'('`, per includere quello che segue fino alla seconda `')'` nel SOA record.

Riga 3: Il serial number è una cifra arbitraria, da aumentare ogni volta che si modifica questo file. Avete bisogno di questa cifra per informare il name server secondario (Slave-Server) delle modifiche che eseguite. Di solito, si usa impiegare un numero a cinque cifre, composto da data e numero da aumentare, nella forma AAAAMMGGNN.

Riga 4: Il refresh rate indica l'intervallo di tempo durante il quale il name server secondario verifica il serial number della zona. In questo caso, si tratta di 1 giorno (1D = 1 day).

Riga 5: Il retry rate indica il lasso di tempo durante il quale il name server secondario cerca di ristabilire il contatto con il server primario, in caso di errore. Si tratta qui di un lasso di tempo di due ore (2H = 2 hours).

Riga 6: L'expiration time indica quanto tempo passa prima che il name server secondario espelli i dati nella cache, qualora non riesca a stabilire un contatto con il server primario. In questo caso, si tratta di una settimana (1W = 1 week).

Riga 7: Il minimum time to live indica per quanto tempo i risultati delle richieste del DNS di altri server debbano restare nella cache, prima di venire invalidati. Nel qual caso bisogna riformulare la richiesta.

Riga 9: L'IN NS indica il name server responsabile per questo dominio. Anche in questo caso, il gateway viene completato automaticamente come gateway.mondo.all, poiché non termina con un punto `'.'`. Di righe come questa, ce ne possono essere parecchie: una per il name server primario e una per ogni secondario. Se, per questa zona, notify su `/etc/named.conf` non sta su no, verrano informati tutti i name server qui elencati delle modifiche dei dati di zona.

Riga 10: L'MX-record indica il mail server che riceve le mail per il dominio mondo.all, per poi elaborarle o inoltrarle. In quest'esempio, si tratta dell'unità sole.mondo.all. Il numero prima del nome del server è il valore di preferenza: in presenza di più MX, si prenderà il mail server con il valore più basso; se la consegna a questo server fallisce, si prova con il server con il valore immediatamente più alto.

Righe 12-17: Gli address-record propriamente detti, quelli in cui il nome di PC viene attribuito ad uno o più indirizzi IP. In questo caso, i nomi vengono riportati senza un punto alla fine, dal momento che sono registrati senza il relativo dominio e deveno essere tutti comunque completati con mondo.all. All'unità gateway sono attribuiti due indirizzi IP, dacché dispone di due schede di rete.

Per il 'reverse lookup' (risoluzione inversa) degli indirizzi IP, che riconduce gli indirizzi IP ai relativi server, si ricorre allo pseudo-dominio in-addr.arpa. Questo dominio viene aggiunto all'elemento di rete scritto alla rovescia. Quindi, 192.168.1 diventa 1.168.192.in-addr.arpa;.

```
1. $TTL 2D
2. 1.168.192.in-addr.arpa. IN SOA gateway.mondo.all. root.mondo.all. (
3.                          2001040901      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS           gateway.mondo.all.
10.
11. 1                       IN PTR          gateway.mondo.all.
12. 2                       IN PTR          terra.mondo.all.
13. 3                       IN PTR          marte.mondo.all.
```

file 39: *Risoluzione inversa dell'indirizzo*

Riga 1: $TTL definisce gli standard TTL validi per tutte le voci.

Riga 2: Questo file permette il 'reverse lookup' per la rete 192.168.1.0. Dal momento che la zona del caso è '1.168.192.in-addr.arpa', non la si vorrà aggiungere al nome del server: per questo motivo, i nomi sono tutti completi di dominio e punto finale. Il resto corrisponde all'esempio dato per mondo.all.

Righe 3-7: vd. esempio di mondo.all.

Riga 9: Questa riga indica di nuovo il name server responsabile per questa zona. Questa volta, però, riporta il nome completo di dominio e punto finale.

Riga 11-13: I pointer-record, che indicano il nome di server relativo ad un determinato indirizzo IP. All'inizio della riga, trovate solo l'ultima parte dell'indirizzo, senza '.'. Se, ora, vi attaccate la zona e fate finta che non ci sia '.in-addr.arpa', avrete l'indirizzo IP completo, scritto alla rovescia.

I dati di zona, in questa forma, sono utilizzabili sia per Bind8 che per Bind9. Anche i trasferimenti di zone tra le diverse versioni non dovrebbero, normalmente, essere un problema.

Ulteriori informazioni

- Documentazione sul pacchetto `bind8`: `file:/usr/share/doc/packages/bind8/html/index.html`.
- Un esempio di configurazione si trova sotto: `/usr/share/doc/packages/bind8/sample-config`
- La pagina di manuale di `named` (`man 8 named`), nella quale vengono nominati RFCs pertinenti, come pure la pagina di manuale di `named.conf` (`man 5 named.conf`).

NIS – Network Information Service

Qualora siano più di un sistema Unix ad accedere a risorse comuni nell'ambito di una rete, si dovrà assicurare che le identità degli utenti e dei gruppi non creino conflitti su nessun computer. La rete deve essere trasparente per tutti gli utenti, in modo che indipendentemente dal computer sul quale l'utente lavori, egli trovi sempre lo stesso ambiente. Questo compito viene svolto dai servizi NIS ed NFS. L'NFS serve alla ripartizione di filesystem nella rete e viene descritto più dettagliatamente nel paragrafo *NFS – filesystem ripartiti* a pagina 245.

NIS (ingl. *Network Information Service*) può essere considerato un servizio di gestione di banche dati, che permette l'accesso alle informazioni dei file `/etc/passwd`, `/etc/shadow` o `/etc/group` da ogni punto della rete. L'NIS può anche essere usato per compiti più complessi (ad esempio, per `/etc/hosts` o `/etc/services`), sui quali, tuttavia, non ci soffermeremo in questa sede. L'NIS è anche conosciuto come `'YP'`, dall'inglese *yellow pages*, ovvero *le pagine gialle* della rete.

Server NIS master e slave

Per installarlo selezionate in YaST2 'Rete/Avanzata' e lì 'Server NIS'.

Se nella vostra rete non vi sono ancora server NIS, alla prossima maschera dovete attivare la voce 'Installa e imposta server NIS master'. Se avete già un server NIS (dunque un "master"), potete aggiungere (per esempio quando configurate una nuova sottorete) un server NIS slave. Iniziamo cola la configurazione del server master. Nella prima maschera di configurazione (Fig. 9.4 nella pagina successiva) immettete in alto il nome di dominio. Nella checkbox (nella parte inferiore) potete stabilire, se il computer debba anche fungere da client NIS, dunque se deve essere possibili che gli utente possano eseguire il login che otterrano i dati anche dal server NIS.

Se in un secondo momento intendete integrare nella vostra rete ulteriori server NIS ("server slave"), dovrete attivare la box 'Esiste un server NIS slave attivo'. In aggiunta va attivata anche la casella 'Distribuzione veloce mappe' che comporta una trasmissione rapida delle registrazione della banca di dati dal master al server slave.

Se volete permettere agli utenti nella vostra rete di modificare le loro password (con il comando `yppasswd`, dunque non solo quelli locali, ma quelli che si trovano sul server NIS), lo potete impostare anche in questa maschera. Si attiveranno anche le checkbox 'Permetti di cambiare il campo GECOS'

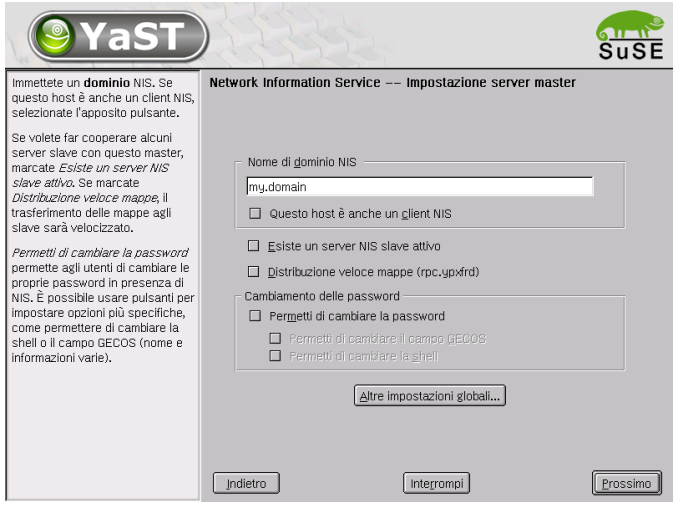


Figura 9.4: *YaST2: tool di configurazione per server NIS*

e 'Permetti di cambiare la shell'. "GECOS" significa che l'utente ha la possibilità di modificare le sue impostazioni del nome e indirizzo (con il comando `ypchfn`). "SHELL" vuol dire che può scegliere un'altra shell di quella di default (con il comando `ypchsh`, per esempio da bash a sh).

Sotto 'Altre impostazioni globali...' appare un menu (Fig. 9.5 nella pagina seguente), in cui si può cambiare la directory sorgente (`/etc`). Inoltre si possono unire password e gruppi. Le impostazioni vanno lasciate su 'Sì', in modo che non si creano delle incongruenze tra i file (`/etc/passwd` e `/etc/shadow` o `/etc/group` e `/etc/gshadow`). Inoltre si può stabilire l'ID minimo degli utente e gruppi. Facendo clic su 'OK', vi ritrovate nella maschera precedente. A questo punto fate clic su 'Prossimo'.

Se prima avete selezionato 'Esiste un server NIS slave attivo', dovete immettere i nomi dei computer che fungeranno da slave. Stabilite il nome è fate clic su 'Prossimo'. Il seguente menu viene raggiunto anche direttamente, se prima non avete attivato l'impostazione per i server slave. Qui potete impostare le "mappe", che dal server NIS devono essere trasferite sui rispettivi client. Nella maggioranza dei casi e di solito si sconsiglia di modificare le preimpostazioni. Se però volete modificarle, dovrete conoscere bene questo campo.

Con 'Prossimo' arrivate all'ultimo dialogo, dove potete stabilire quali re-

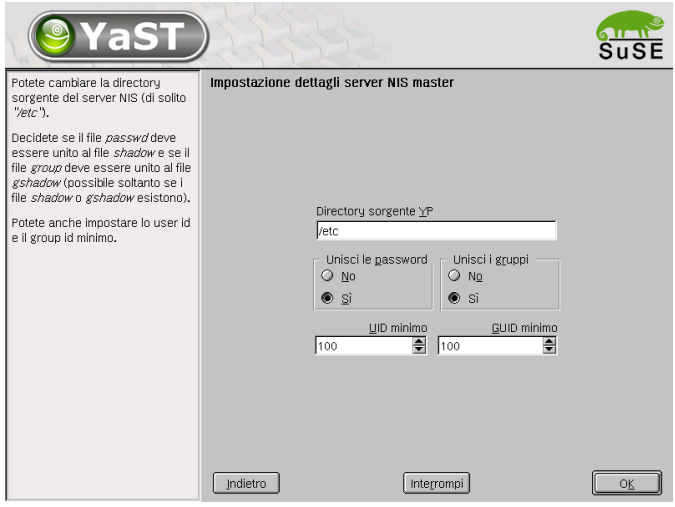


Figura 9.5: *YaST2: server NIS: modificare directory e sincronizzare file*

te possono interrogare il server NIS (vd. Fig. 9.6 a pagina 243). Di solito si tratta della rete aziendale, in questo caso dovrebbero esserci le registrazioni

```
255.0.0.0 127.0.0.0
0.0.0.0 0.0.0.0
```

La prima permette connessioni dal proprio computer, e la seconda permette a tutti i computer con accesso alla rete di interrogare il server.

Il modulo client NIS in YaST2

Questo modulo vi permette di configurare facilmente il client NIS. Nella prima finestra per l'impostazione del NIS indicate che volete utilizzare NIS. Nel dialogo successivo indicate il nome di dominio NIS e il numero IP del server NIS.

Con la checkbox 'Broadcast' permettete la ricerca di un server NIS all'interno della rete, se il server indicato non dovesse rispondere. Avete anche la possibilità, di indicare domini multipli con un dominio di default. Per i singoli domini poi, con 'Aggiungi' potete indicare più server inclusa la funzione broadcast.

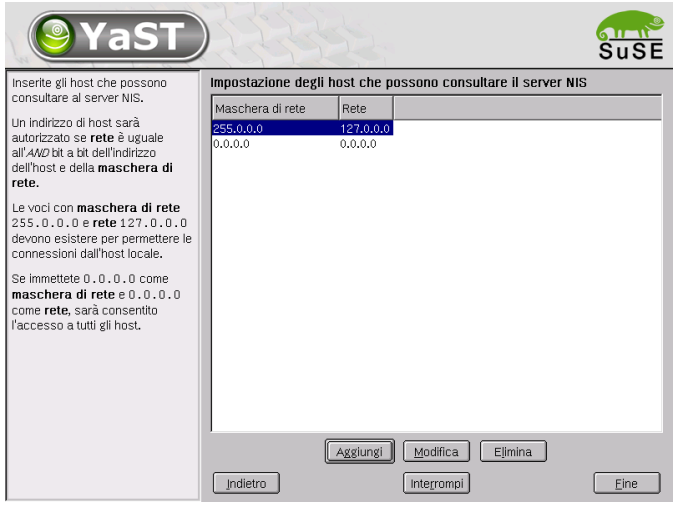


Figura 9.6: *YaST2: server NIS: impostazione degli host che possono consultare il server*

Configurazione manuale di un client NIS

Nel pacchetto `ypbind`, troverete tutti i programmi necessari alla configurazione di un client NIS. Essenziali sono i seguenti passi:

- Inserite il dominio NIS nel file `/etc/defaultdomain`. Il nome del dominio NIS non va confuso con il nome del dominio DNS . Anche se sono uguali, l'uno non ha niente a che vedere con l'altro!
- Inserite il nome del server NIS nel file`/etc/yp.conf`:

  ```
  ypserver 192.168.0.1
  ```

- Il nome del server NIS (per esempio, `sole.cosmo.com`) deve poter essere risolvibile tramite `/etc/hosts`.
- L'NIS viene realizzato tramite RPC (ingl. *Remote Procedure Calls*), ragion per cui è necessario attivare il portmapper RPC. Questo server viene avviato dallo script `/etc/init.d/portmap`.
- Completate le registrazioni in `/etc/passwd` ed `/etc/group`. . Per far sì che alla fine della ricerca tra i file locali venga inviata una richiesta

al server NIS, ai rispettivi file va aggiunta una riga che inizia con un segno del più (`'+'`).

- NIS prevede anche una serie di altre opzioni, da attivare nel file `/etc/sysconfig/ypbind`.
- L'ultimo passo della configurazione del client NIS consiste nel lanciare il programma ypbind, ovvero il client NIS propriamente detto.
- Riavviate il sistema oppure riavviate i servizi necessari con i seguenti comandi:

```
terra:   #  rcnetwork restart
terra:   #  rcypbind restart
```

NFS – filesystem ripartiti

Come abbiamo già accennato nel paragrafo 9 a pagina 240, l'NFS e l'NIS servono a rendere la rete trasparente all'utente. L'NFS permette di ripartire i filesystem nella rete. A prescindere dal computer sul quale l'utente lavorari, egli troverà sempre lo stesso ambiente.

Sia l'NIS, che l'NFS sono servizi asimmetrici. C'è un server NFS ed un client NFS, ma ogni computer può essere contemporareamente sia l'uno che l'altro, ovvero può collocare filesystem nella rete ("esportare"), e montare filesystem di altri computer ("importare"). Normalmente, tuttavia, si usano a questo scopo dei server con hard disk capienti, i cui filesystem vengono poi montati dai client.

Importare filesystem con YaST2

Ogni utente (se dispone dei relativi permessi), può montare directory NFS di server NFS nel proprio albero di file. Il modo più semplice è farlo con il modulo 'Client NFS' in YaST2. Dovete solo immettere l'hostname del computer che funge da server NFS, la directory da esportare e il punto di montaggio sul proprio computer. Nella prima finestra di dialogo selezionate 'Aggiungi' ed immettete le indicazioni di cui sopra (vd. Fig. 9.7).

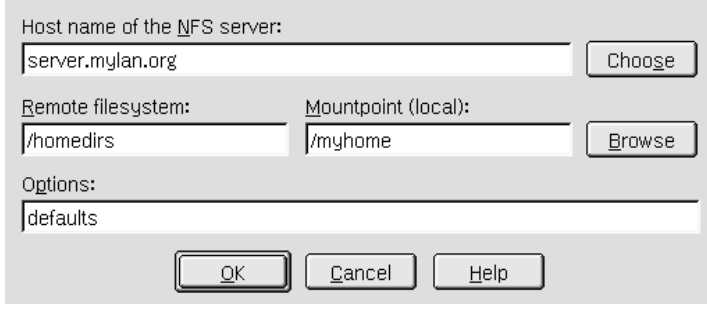


Figura 9.7: *Configurare il client NFS*

Importare manualmente i filesystem

Importare i filesystem di un server NFS è molto facile. L'unico requisito è che sia stato prima avviato il portmapper RPC . Abbiamo già visto come lan-

ciare questo server quando abbiamo parlato dell'NIS (vd. sezione 9 a pagina 243). Dopodiché sarà possibile includere filesystem estranei nel proprio filesystem (a condizione che essi siano stati esportati dai relativi computer) in modo analogo ai dischi locali, ovvero con il comando `mount`. La sintassi è la seguente:

`mount -t nfs` ⟨*`Computer`*⟩`:`⟨*`Percorso remoto`*⟩ ⟨*`Percorso locale`*⟩

Per importare, ad esempio, le directory dell'utente dal computer `sole`, usate il comando:

```
terra:~ #  mount -t nfs sole:/home /home
```

Esportare filesystem con YaST2

YaST2 vi permette di trasformare in poco tempo un computer della vostra rete in un server NFS: un server che mette a disposizioni directory e file a tutti i computer con permesso di accesso. Gli utenti possono usufruire così di applicativi senza doverli installare localmente sul loro computer.

Per eseguire l'installazione selezionate in YaST2: 'Rete/Avanzata' e lì 'Server NFS' .

Quindi, selezionate 'Avvia server NFS' e fate clic 'Prossimo'

Nella casella superiore immette le directory da esportare, e in quella inferiore i computer della vostra rete con il permesso di montarle (Fig. 9.8 nella pagina successiva). Per ogni computer possono essere settate quattro opzioni, ⟨*host singolo*⟩, ⟨*gruppi di rete*⟩, ⟨*wildcards*⟩ e ⟨*reti IP*⟩. Una descrizione dettagliata di queste opzioni si trova nelle pagine di manuale per pacchetto `exports` (`man exports`).

Con 'Fine' concludete la configurazione.

Esportare manualmente i filesystem

Su un server NFS devono essere inizializzati i seguenti server di rete:

- Il portmapper RPC (portmap)
- L'RPC-mount-daemon (rpc.mountd)
- RPC-NFS-daemon (rpc.nfsd)

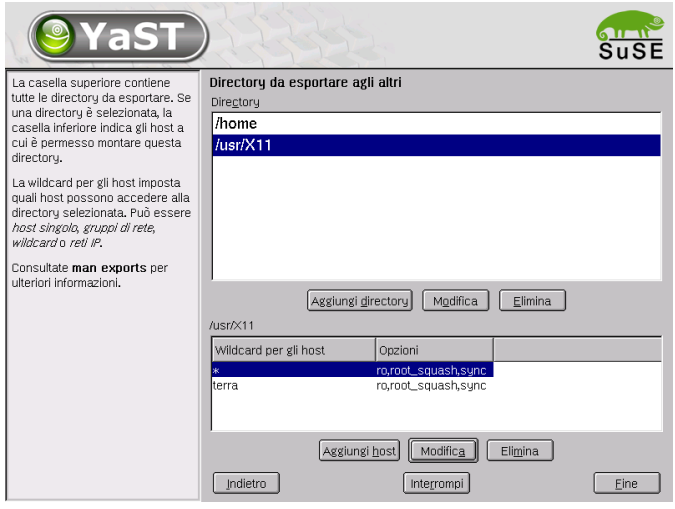


Figura 9.8: *YaST2: server NFS: immettere directory da esportare e host*

Essi vengono avviati al boot del sistema dagli script `/etc/init.d/portmap` ed `/etc/init.d/nfsserver`.

Inoltre,dovrà essere specificato quali filesystem debbano essere esportati a quale computer. Ciò avviene nel file `/etc/exports`.

Ogni directory da esportare ha bisogno di una riga che descriva quali computer possano avere accesso a queste informazioni. Anche tutte le sottodirectory di un indirizzario esportato vengono esportate automaticamente. I computer che possono accedervi sono solitamente contrassegnati dai propri nomi (compreso il nome del dominio), ma è anche possibile contrassegnarli con i simboli jolly `'*'` e `'?'`, con tutte le funzioni che abbiamo imparato a conoscere nell'ambito di bash. Se non indicate alcun nome, saranno tutti i computer ad avere accesso a questa directory (con i diritti da voi impostati).

I diritti con i quali una directory viene esportata vengono riportati nella lista tra parentesi, dopo il nome del computer. I più importanti diritti di accesso sono descritti nella tabella successiva:

Opzioni	Significato
ro	Il filesystem viene esportato solo con diritti di lettura (default).

Tabella 9.12: *Continua alla pagina seguente...*

rw	Il filesystem viene esportato con diritti di lettura e scrittura.
root_squash	Questa opzione fa sì che l'utente `root` del computer in questione non disponga dei normali diritti `root` per questo filesystem. Per attivare questa opzione, l'accesso con l'user-ID `0` viene trasferito all' user-ID `65534 (-2)`, che dovrebbe a sua volta essere attribuito all'utente`nobody` (default).
no_root_squash	I diritti di accesso di root non vengono trasferiti e restano quindi invariati.
link_relative	Questa opzione converte i link assoluti e simbolici (ovvero tutti quelli che iniziano con `'/'`) in una sequenza di `'../'`. È un'opzione utile solo quando venga montato l'intero file system di un computer (default).
link_absolute	I link simbolici restano invariati.
map_identity	Sul client, vengono usate le stesse user-ID del server (default).
map_daemon	client e server non hanno le stesse user-ID. Con questa opzione, nfsd riceve l'istruzione di creare una tabella di conversione per le user-ID, a condizione che abbiate attivato il daemon ugidd.

Tabella 9.12: *Diritti di accesso a directory esportate*

Il file `exports` potrebbe, ad esempio, essere simile al file 40.

```
#
# /etc/exports
#
/home            sole(rw)   venere(rw)
/usr/X11         sole(ro)   venere(ro)
/usr/lib/texmf   sole(ro)   venere(rw)
/                terra(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

file 40: *`/etc/exports`*

Il file `/etc/exports` viene letto da mountd e nfsd. Se viene anche modificato, sia mountd, che nfsd devono essere riavviati, in modo che questa modifica venga validata. Per riavviare i due programmi, digitate:

```
terra:~ #  rcnfsserver restart
```

DHCP

Il protocollo DHCP

Il cosiddetto “Dynamic Host Configuration Protocol” serve ad assegnare – da un server centrale – impostazioni in una rete invece di configurarle in modo decentrato sui singoli computer. Un client configurato con DHCP non dispone di indirizzi statici, ma si configura in modo completamente autonomo secondo le indicazioni del server DHCP.

Inoltre è possibile identificare ogni client sulla base dell’indirizzo hardware (quasi sempre definito permanentemente) della sua scheda rete e munirlo costantemente con le stesse impostazioni, come pure assegnare gli indirizzi di un determinato pool “dinamico” ad ogni computer “interessato”. In questo caso, il server DHCP provvederà a far sì che ad ogni client – per tutte le esigenze – venga assegnato lo stesso indirizzo (anche per lunghi periodi di tempo) – naturalmente, questo non funziona se nella rete ci sono più computer che indirizzi.

Un amministratore del sistema può quindi approfittare in due modi di DHCP. Da un DHCP è possibile eseguire comodamente vaste modificazioni degli indirizzi e configurazione della rete senza dover configurare singolarmente una quantità di client, e d’altra parte, specialmente i nuovi computer, possono venire facilmente integrati nella rete assegnando loro un numero IP dal pool di indirizzi. Anche per i laptop, che vengono regolarmente usati in diverse reti, è certamente interessante poter percepire – da un server DHCP – di volta in volta l’impostazione rete adeguata.

Oltre all’indirizzo IP e alla maschera rete, vengono comunicati al client anche il nome del computer e del dominio del gateway ed degli indirizzi del server dei nomi che devono venire utilizzati. Oltre a ciò possono venire configurati centralmente anche molti altri parametri come p.e. un print server o un time server da cui è possibile richiedere l’ora attuale. In quel che segue, vi forniremo una breve descrizione di DHCP. Desideriamo soprattutto usare il server DHCP, dhcpd, per mostrarvi come sia facile eseguire centralmente, anche nella vostra rete, una completa configurazione della rete.

I pacchetti software DHCP

Su SuSE Linux sono contenuti tre importanti pacchetti per DHCP.

A questo punto, dovremmo menzionare il server DHCP `dhcpd` a cura dell’ Internet Software Consortium che assegna ed amministra nella rete le rispettive impostazioni. Ma, mentre normalmente in SuSE Linux viene usato solo

dhcpd come server, come client DHCP si può scegliere fra due alternative. Anche qui dobbiamo fare cenno al dhclient (anche questo a cura dell'ISC), senza tralasciare però il cosiddetto "DHCP Client Daemon" contenuto nel pacchetto dhcpcd.

Il dhcpcd installato come standard su SuSE Linux, è molto semplice da usare e viene automaticamente avviato – per la ricerca di un server DHCP – allo start del computer. Se la cava senza un file di configurazione e normalmente dovrebbe funzionare senza altre configurazioni.

Per situazioni più complesse, si può ricorrere al dhclient ISC, che può venire configurato tramite il file di configurazione /etc/dhclient.conf. Sia che debba venire aggiunto un ulteriore domain nell'elenco di ricerca, sia che debba venire emulato il comportamento di un client DHCP di Microsoft, l'utente esperto ha a disposizione innumerevoli possibilità di adattare alle sue esigenze, fin nei minimi particolari, il comportamento del dhclient.

Il server DHCP, dhcpd

Il *Dynamic Host Configuration Protocol Daemon* è il nocciolo di ogni sistema DHCP. Egli "affitta indirizzi" e ne sorveglia l'uso come stabilito nel file di configurazione /etc/dhcpd.conf. Tramite i parametri e i valori lì definiti, l'amministratore dispone di una quantità di mezzi che gli permettono di influenzare il DHCP secondo i suoi bisogni.

Esempio di un semplice file /etc/dhcpd.conf:

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "cosmo.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

file 41: *Il file di configurazione* /etc/dhcpd.conf

Questo semplice file di configurazione è sufficiente affinchè DHCP sia in grado di attribuire indirizzi nella vostra rete. Fate specialmente attenzione ai punti e virgola alla fine di ogni riga; senza di essi, dhcpd non verrà avviato!

Come vedete, il nostro esempio può venire suddiviso in tre blocchi.

Nel primo blocco viene definito per quanti secondi (impostazione standard) un indirizzo IP venga "affittato" ad un computer richiedente, prima che questi cerchi di avere una proroga (`default-lease-time`). Qui viene anche indicato il periodo massimo per il quale un computer può tenere il numero IP assegnatogli dal server DHCP, senza dover richiedere una dilazione di tempo (max-lease-time).

Nel secondo blocco vengono definiti globalmente alcuni parametri di rete fondamentali:

- Con `option domain-name` viene definito il dominio preimpostato della vostra rete.
- Con `option domain-name-server` possono venire indicati fino a tre server DNS che devono venire utilizzati per la risoluzione di indirizzi IP in host name (e viceversa). Sarebbe naturalmente ideale, se nel vostro sistema o entro la vostra rete, fosse già in uso un server dei nomi che tiene pronto un host name anche per gli indirizzi dinamici e viceversa. Ulteriori informazioni riguardanti la creazione di un proprio server dei nomi vedi sezione 9 a pagina 230.
- `option broadcast-address` stabilisce quale indirizzo broadcast debba usare il computer richiedente.
- `option routers` stabilisce dove debbano venire inviati quei pacchetti di dati che – a causa dell'indirizzo mittente e ricevente e della maschera della sottorete – non possono venire consegnati nella rete locale. Nella maggior parte dei casi, proprio nelle reti minori questo router è anche il passaggio ad internet.
- `option subnet-mask` indica la maschera rete da consegnare al client.

Al di sotto di queste impostazioni generali, viene definita un'altra rete con la maschera-sottorete. Infine deve venire scelta anche un'area indirizzi dalla quale il daemon DHCP possa attribuire indirizzi ai client richiedenti. Nel nostro esempio, sono disponibili tutti gli indirizzi fra `192.168.1.10` e `192.168.1.20` oppure `192.168.1.100` e `192.168.1.200`.

Dopo queste poche righe, dovreste già essere in grado di attivare, con il comando `rcdhcpdstart`, il daemon DHCP che sarà subito a vostra disposizione. Con `rcdhcpd syntax-check` potete anche far eseguire un breve controllo del file di configurazione. Se, contro ogni aspettativa, dovessero esserci dei problemi con la configurazione, ed il server dovesse terminare con un errore invece di iniziare con un done, troverete informazioni a riguardo, sia nel file centrale di protocollo del sistema `/var/log/messages`, sia sulla console 10 (Ctrl + Alt + F10).

Computer con indirizzo IP fisso

Dopo essere riusciti a configurare il server per l'attribuzione degli indirizzi dinamici, vogliamo osservare un po' più da vicino l'attribuzione di indirizzi *statici*. Come già accennato all'inizio, con DHCP è possibile assegnare allo stesso computer e ad ogni richiesta, un determinato indirizzo.

Naturalmente tali esplicite attribuzioni di indirizzi hanno la precedenza sulle attribuzioni degli indirizzi dinamici presi dal pool. Al contrario degli indirizzi dinamici, le informazioni fisse degli indirizzi non vengono cancellate se non ci sono più indirizzi liberi disponibili che rendono necessaria una nuova distribuzione.

Per l'identificazione di un sistema definito con un indirizzo *statico*, DHCPD si serve del cosiddetto indirizzo hardware: si tratta di un numero fisso unico (generalmente) al mondo formato da sei paia di ottetti assegnato ad ogni dispositivo di rete, p.e. `00:00:45:12:EE:F4`.

Se il file di configurazione della figura 1 viene completato con la registrazione della figura 2, DHCPD fornirà sempre gli stessi dati al computer corrispondente.

```
host terra {
  hardware ethernet 00:00:45:12:EE:F4;
  fixed-address 192.168.1.21;
}
```

file 42: *Completare il file di configurazione*

La struttura di queste righe parla da sé:

Prima viene registrato il nome DNS del computer da determinare (host *hostname*) e nella riga seguente viene definito l'indirizzo MAC. Nei sistemi Linux, potete trovare questo indirizzo con il comando `ifstatus` assieme al nome della scheda di rete (ad esempio, eth0). Può darsi che abbiate prima bisogno

di attivare la scheda: `ifup eth0`. Otterrete un output del tipo: *link/ether 00:00:45:12:EE:F4*.

Nel nostro esempio, viene assegnato al computer (la cui scheda rete possiede l'indirizzo MAC *00:00:45:12:EE:F4*) l'indirizzo IP `192.168.1.21` ed il nome `terra`.

Oggigiorno, come tipo di *hardware* viene generalmente usato `ethernet`, ma viene anche supportato `token-ring`, usato per la maggior parte nei sistemi IBM.

Ulteriori fonti di informazione

Come già accennato all'inizio, vogliamo offrirvi solo un sommario delle funzioni DHCP. Se siete interessati ad altre informazioni, andate p.e. alla pagina dell'*Internet Software Consortium* (`http://www.isc.org/products/DHCP/`) su cui avrete a disposizione ulteriori informazioni su DHCP: in questa pagina viene documentata anche la versione 3 (al momento ancora versione Beta) del protocollo. Naturalmente avete a disposizione anche le man page e specialmente `man dhcpd`, `man dhcpd.conf`, `man dhcpd.leases` e `man dhcp-options` e nelle librerie troverete alcuni libri che si occupano delle possibilità del *Dynamic Host Name Configuration Protocol*.

Inoltre `dhcpd` è perfino in grado di offrire ai computer richiedenti, un file – contenente un kernel avviabile del sistema operativo – definito nel file di configurazione con il parametro *filename*. In questo modo è possibile creare client, che non contengono alcun disco rigido e che caricano sia il loro sistema operativo come pure i loro file eclusivamente tramite la rete (*diskless clients*). La cosa può essere interessante sia sotto il punto di vista dei costi che sotto il punto di vista della sicurezza.

Reti eterogenee

In questo capitolo vi mostriamo come far comunicare il vostro sistema Linux con Windows e/o Macintosh.

Samba 256
Netatalk 263

Samba

Con Samba è possibile trasformare un qualsiasi computer Unix in un file e print server performante per computer DOS, Window ed OS/2: Il progetto Samba viene curato dal Samba Team ed è stato sviluppato dall'australiano Andrew Tridgell.

Samba è ormai un prodotto maturo, e per questo motivo possiamo solo trattare brevemente alcune funzionalità. Comunque il software viene fornito con una completa documentazione in forma digitale composta da una parte da pagine di manuale — a causa del volume chiamate `apropos samba` con la riga di comando — e dall'altra da documentazione ed esempi che trovate sotto `/usr/share/doc/packages/samba`, dopo aver installato Samba. Nella sottodirectory `examples` trovate anche l'esempio di configurazione commentato `smb.conf.SuSE`.

Samba utilizza il protocollo SMB (Server Message Block) della Microsoft, che si basa sui servizi di NetBIOS. Cedendo alle richiesta di IBM, la Microsoft ha pubblicato il protocollo in modo da permettere anche ad altri fornitori di software di creare delle connessioni alla rete di dominio della Microsoft. Samba imposta il protocollo SMB su TCP/IP. Così su ogni client deve essere installato il protocollo TCP/IP. Noi consigliamo di utilizzare solo TCP/IP sui client.

NetBIOS

NetBIOS è un'interfaccia software (API) progettata per la comunicazione tra computer; viene messo a disposizione un servizio del nome (ingl. *name service*) ai fini della identificazione reciproca dei computer. Non vi è una istanza centrale ad assegnare i nomi, ogni computer nella rete può riservarsi un nome non ancora assegnato. L'interfaccia di NetBIOS può venire implementata su diverse architetture di rete. Un'implementazione che lavora a stretto contatto con l'hardware si chiama NetBEUI. NetBEUI viene spesso chiamata NetBIOS.

Altri protocolli di rete con cui è stato implementato NetBIOS sono IPX di Novell e TCP/IP.

I nomi NetBIOS che vengono anche assegnati all'implementazione di NetBIOS tramite TCP/IP non hanno niente a che vedere con i nomi assegnati nel file `/etc/hosts` o via DNS – NetBIOS usa propri "name space" (area in cui sono validi i nomi). Per semplificare l'amministrazione è però consigliabile assegnare almeno ai server nomi NetBIOS che corrispondano al loro DNS-hostname: su Samba, ciò avviene di default.

Client

Tutti i comuni sistemi operativi per PC, come DOS, Windows e OS/2, supportano il protocollo SMB. Sul computer deve essere installato il protocollo TCP/IP. Per le diverse versioni UNIX si può usare anche Samba.

I server SMB mettono a disposizione dei loro client spazi dell'hard disk in forma di cosiddette "Share". Una share comprende una directory con tutte le sottodirectory sul server; viene esportata con un nome e può venire indirizzata dai client con questo nome. A questo scopo, il nome della share può essere assegnato liberamente. Non deve corrispondere al nome della directory esportata. Allo stesso modo viene attribuito un nome ad una stampante esportata, tramite il quale i client vi possono accedere.

Installazione e configurazione del server

Installate il pacchetto `samba` della serie `n`. Poi, avviate manualmente i servizi con il comando `rcsmb start`; per terminarli, digitate `rcsmb stop`.

Il file di configurazione centrale di Samba è `/etc/samba/smb.conf`. Essenzialmente, il file di configurazione `/etc/samba/smb.conf` si divide in due sezioni. Nella cosiddetta sezione [globals] avvengono le impostazioni centrali e generali. La seconda sezione viene chiamata [share]. Qui vengono definite le singole share per file e stampante. I dettagli della share possono essere impostati singolarmente o uniforme per tutti nella sezione [global]. Ciò risulta in una maggior chiarezza per quanto riguarda i file di configurazione. Visto che durante il funzionamento, questo file viene spesso utilizzato, un breve file di configurazione senza commenti comporterà dei miglioramenti per quanto riguarda le modalità di risposta e di reazione del server Samba.

I parametri selezionati vengono spiegati in seguito.

Sezione global in base alla configurazione esempio

I seguenti parametri della global section devono essere adattati alle caratteristiche della vostra rete, affinché il vostro server Samba sia indirizzabile per SMB da altri sistemi in una rete Windows.

- workgroup = gruppo_di_lavoro TUX-NET Il server Samba viene assegnato ad un gruppo di lavoro attraverso questa riga. Adattate TUX-NET ai gruppi di lavoro esistenti o configurate i client secondo i valori qui selezionati. Il server Samba in questa configurazione è visibile con un nome DNS nel gruppo di lavoro selezionato, se il nome non è ancora disponibile.

Se il nome è già stato assegnato, con `netbiosname=MIONOME` può essere impostato un nome che differisce dal nome DNS. I dettagli di questi parametri si possono reperire con `man smb.conf`.

- os level = 2 In base a questo parametro il server Samba decide se tentare di fungere da LMB (ingl. *Local Master Browser*) per il proprio gruppo di lavoro. Il valore utilizzato nell'esempio è stato scelto volutamente basso, per evitare che una rete Windows venga disturbata da un server Samba configurato in modo errato. I dettagli su questo tema importante si trovano nei file BROWSING.txt e BROWSING-Config.txt nella sottodirectory `textdocs` della documentazione del pacchetto.

  Se un server SMB — per esempio Windows NT, 2000 Server — è già in funzione ed il server Samba dovrà mettere a disposizione nella rete locale i nomi di sistemi disponibili, aumentate il valore dell'os level (per esempio 65), per vincere la gara per diventare il LMB.

  Siate cauti nel modificare questo valore, poiché potreste causare dei malfunzionamenti in una rete Windows. Consultatevi con il vostro amministratore di sistema, testate prima le modifiche in una rete isolata od in un momento poco critico.

- wins support e wins server Volete integrare un server Samba in una rete Windows esistente, con un server WINS: per fare questo dovete attivare il parametro wins server cancellando il punto e virgola e adattare di conseguenza l'indirizzo IP.

  I sistemi Windows che sono in esecuzione in sottoreti separate, devono essere visibili tra di loro, dato che nella vostra rete Windows *non* vi è un server WINS ed il vostro server Samba deve assumere il ruolo di server WINS: per fare questo attivate la riga con wins support = yes. Assicuratevi assolutamente che questo parametro sia attivato solo su un server Samba. Inoltre in questa constellazione il server wins deve essere disattivato.

Shares

Nei seguenti esempi vengono sharati da una parte i lettori CD-ROM e dall'altra le directory di coloro che utilizzano, homes per client SMB.

CD-ROM

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = no
```

file 43: *Sharare CD-ROM*

Per evitare di sharare inavvertitamente un CD-ROM, tutte le righe necessarie per questa share sono disattivate.

- [cdrom] e comment [cdrom] è il nome share visibile ai client SMB. Con comment si può comunicare ai client una denominazione espressiva della share.
- path = `/media/cdrom` con `path` si esporta la directory `/media/cdrom`.

Questo tipo di share è disponibile solo per gli utenti presenti nel sistema per motivi di una impostazione di default volutamente restrittiva. Se la share deve essere disponibile a tutti, bisogna aggiungere la riga guest ok = yes. Visto che ognuno ha il permesso di lettura, questa impostazione dovrebbe essere maneggiata con estrema cautela, ed applicarla solo per share scelte. Particolare cautela vale per l'utilizzo di questa impostazione nella [global] section.

Per la share di [homes] vale: se un utente ha sul server file Linux un valido account ed una propria directory Home, immettendo un login e una password valida il suo client può collegarsi con questo.

```
[homes]
        comment = Home Directories
        valid users = %S
        browseable = no
        writeable = yes
        create mask = 0640
        directory mask = 0750
```

file 44: *Sharare homes*

- [homes] Se non esiste una esplicita share con il nome share dell'utente che si connette, viene generata dinamicamente una share in base alla share [homes]. Il nome della share è identico a quello del utente.

- valid users = %S %S viene sostituito dal nome della share una volta stabilito il collegamento. Visto che con la share [homes] questo è identico al nome dell'utente, gli utenti ammessi vengono limitati ai proprietari della directory utente. Questa è una possibilità per consentire l'accesso solo ai proprietari.

- browseable = no con questa impostazione la share [homes] non è visibile nell'elenco delle share.

- writeable = yes di default, Samba proibisce l'accesso in scrittura su share esportate read only = yes. Se un indirizzario deve poter essere accessibile alla scrittura, impostare il valore writeable = yes. Nel caso di directory di utente questo di solito è auspicato.

- create mask = 0640 I computer Windows non conoscono il concetto dei diritti d'accesso di Unix; non possono perciò indicare, alla creazione di file, quali diritti d'accesso essi abbiano.
  Il parametro create mask stabilisce con quali diritti di accesso debbano venire creati i file. Questo vale solo per Shares scrivibili. In altre parole, al proprietario viene dato il permesso di lettura e scrittura ed ai membri dello stesso gruppo il permesso di lettura. Ricordate che valid users = %S non concede neanche il permesso di lettura ai membri del gruppo.

Security Level

Il protocollo SMB ha le sue origini nel mondo di DOS e tiene direttamente in considerazione il problema della sicurezza. Ogni accesso ad una share può venire protetto da una password. SMB conosce due diverse possibilità per attuare ciò:

- Share Level Security: Nel Share Level Security viene attribuita una password ad una share. Chi la conosce, ha accesso alla share.

- User Level Security: Questa variante introduce in SMB il concetto di utente. Ogni utente deve fare il login nel server con una password. Dopo di ciò il server può, secondo il nome dell'utente, accordare l'accesso alle singole share esportate.

- Server Level Security: Di fronte al client, Samba sostiene di lavorare in User Level Mode. In verità trasmette tutte le richieste di password ad un altro User Level Mode Server il quale si assume il compito dell'autentificazione. Questa configurazione esige un ulteriore parametro (password server =).

La distinzione fra Share e User Level Security deve venire fatta per tutto il server. Non è possibile esportare singole share via Share Level Security e altri via User Level Security

Per ulteriori informazioni leggete il file `textdocs/security_level.txt`.

Suggerimento

Per una facile amministrazione del server di Samba, c'è anche il programma swat. Mette a disposizione una semplice interfaccia web con la quale potete comodamente configurare il server di Samba. Nell'URL di un browser, inserite `http://localhost:901` e fate il login come utente root. Badate che swat è ora attivo anche nei file `/etc/inetd.conf` e `/etc/services`. Per maggiori informazioni sul programma swat consultate pagina di manuale di `swat` (`man swat`).

Suggerimento

Samba come server per il login

Nelle reti in cui si trovano principalmente windows client, è spesso auspicabile che gli utenti possano fare il login solo con account e password validi. Questo può venire realizzato con l'aiuto di un server Samba. In una rete puramente Windows, un server Windows-NT si assume questo compito; esso è configurato come cosiddetto Primary Domain Controller (PDC). Nella sezione [globals] di `smb.conf` dovrete impostare i seguenti parametri, come nell'esempio 45:

```
[global]
 workgroup = TUX-NET
 domain logons = yes
 domain master = yes
```

file 45: *Global-Section in smb.conf*

Se per la verifica vengono usate password cifrate, il server di Samba deve venire configurato in modo da poterle utilizzare. La registrazione encrypt passwords = yes nella sezione [globals] consente ciò: inoltre gli account e le password degli utenti devono venire convertiti in una forma cifrata conforme a Windows. Questo avviene con il smbpasswd -a name. Poiché secondo il concetto di dominio di Windows NT, anche i computer necessitano di un account di dominio, questo viene creato con i seguenti comandi:

```
useradd nome-del-computer$
smbpasswd -a -m nome-del-computer
```

file 46: *Creare un account macchina*

Con useradd è stato aggiunto un simbolo del dollaro. Il comando smbpasswd lo aggiunge da sé quando si usa il parametro -m.

Nella configurazione esempio commentata vi sono delle impostazioni che automatizzano questi processi.

```
add user script = /usr/sbin/useradd -g machines \
                  -c "NT Machine Account" -d \
                  /dev/null -s /bin/false %m$
```

file 47: *Creare automaticamente un account macchina*

Installazione dei client

Per primo, ricordiamo che i client possono raggiungere il server di Samba solo tramite TCP/IP. NetBEUI o NetBIOS via IPX non sono al momento utilizzabili con Samba; e poiché TCP/IP sta diventando lo standard dappertutto, persino su Novell e Microsoft, è dubbio che questo possa mai cambiare.

Windows 9x/ME

Windows 9x/ME ha già in sé il supporto per TCP/IP. Come per Windows for Workgroups questo non viene però installato con l'installazione standard. Per installare successivamente TCP/IP, si seleziona TCP/IP di Microsoft in 'proprietà' di 'risorse rete', 'aggiungere...' alla voce 'Protocolli'. Fate attenzione all'indicazione corretta del vostro indirizzo rete e della maschera rete! Dopo un reboot del computer Windows, ritroverete il server-samba (configurato

correttamente) nell'ambiente rete. (Doppio clic sull'icona corrispondente sul desktop).

Suggerimento

Per usare una stampante sul server Samba si dovrebbe installare il driver di stampante PostScript di Apple o generico della relativa versione Windows; si consiglia di collegare la queue della stampante Linux che contiene il rilevamento automatico apsfilter.

Suggerimento

Ottimizzazione

Una possibilità di apportare delle ottimizzazioni è rappresentata da socket options. Le impostazioni di default nella configurazione esempio fornita a corredo si orienta ad una rete Ethernet locale. Ulteriori dettagli in pagina di manuale di `smb.conf` (`man smb.conf`) nella sezione socket options e per pagina di manuale di `socket(7)` (`man socket(7)`). Ulteriori approcci vengono descritti in `textdocs/Speed.txt` e `textdocs/Speed2.txt`.

La configurazione di default in `/etc/samba/smb.conf` cerca di proporre dei valori appropriati e ignora le impostazioni che corrispondono ai alle preimpostazioni del Samba-Team, che comunque si lascia realizzare molto difficilmente od è addirittura impossibile soprattutto riguardo alla configurazione di rete e il nome del gruppo di lavoro. Nella configurazione esempio commentata in `examples/smb.conf.SuSE` trovate tante indicazioni utili per gli adattamenti alla vostre esigenze locali.

Suggerimento

Il Samba-Team fornisce con `textdocs/DIAGNOSIS.txt` istruzioni da seguire passo dopo passo controllare la configurazione.

Suggerimento

Netatalk

Con il pacchetto `netatalk`, potrete realizzare un potente server per file e stampante su client OS per Mac: è possibile accedere da un Macintosh ai dati di un computer Linux o stamparli con una stampante collegata.

Netatalk è un pacchetto di programmi Unix che utilizza il DDP (Datagram Delivery Protocol) implementato nel kernel e che implementano il gruppo

di protocolli AppleTalk (ADSP, ATP, ASP, RTMP, NBP, ZIP, AEP e PAP). In principio, Appletalk è un equivalente del molto più diffuso TCP (Transmission Control Protocol). Molti servizi basati su TCP/IP, p.e. per la risoluzione di host name e sincronizzazione del tempo, trovano sotto AppleTalk il loro corrispondente. Al posto di `nslookup` (DNS, Domain Name Service), viene usato il comando `nbplkup` (NBP, Name Binding Protocol) e al posto di `ping` (ICMP ECHO_REQUEST, Internet Control Message Protocol) viene usato il comando `aecho` (AEP, AppleTalk Echo Protocol).

Normalmente, sul server vengono avviati i seguenti tre daemon:

- Il atalkd ("AppleTalk-Network-Manager"), che corrisponde approssimativamente ai programmi ifconfig e route;
- afpd (AppleTalk Filing Protocol daemon), che mette a disposizione per i client Macintosh un'interfaccia ai filesystem di Unix;
- papd (Printer Access Protocol daemon), che mette a disposizione la stampante nella rete (AppleTalk).

Potete esportare senza problemi indirizzari sul server (utile soprattutto in ambienti di reti eterogenee) e non solo tramite Netatalk, ma contemporaneamente anche con Samba (per i client di Windows vd. il capitolo precedente) e NFS (vd. 9 a pagina 245) Backup ed amministrazione dei permessi degli utenti si lasciano eseguire centralmente sul server Linux.

Considerate che:

- a causa di una restrizione dei client Macintosh, le password degli utenti sul server possono avere al massimo 8 caratteri
- i client Macintosh non possono accedere ai file di Unix con più di 31 caratteri
- i file name non possono contenere due punti (`':'`) perché questi, sotto Mac OS, servono come separatori nei nomi dei percorsi.

Il `netatalk` è da installare.

Configurazione del file server

Nella configurazione standard, per gli utenti registrati, "Netatalk" è già funzionante al 100% come file server. Per poter usufruire delle sue proprietà, dovrete eseguire alcune impostazioni nei file di configurazione che troverete nell'indirizzario `/etc/atalk`.

Tutti i file di configurazione sono puri file di testo. Le righe con un rombo `'#'` iniziale e le righe vuote vengono ignorate ("commenti").

Configurare la rete – atalkd.conf

Su `/etc/atalk/atalkd.conf` viene definito tramite quali interfacce vengano offerti i servizi. Nella maggior parte dei casi, si tratta di `eth0`, e qui è sufficiente l'impostazione di un unico valore.

```
eth0
```

(come nel file-esempio). Configurate qui altre interfacce, p.e. nel caso che usiate contemporaneamente più schede di rete. Se viene inizializzato il server, questi cerca nella rete le zone e i server già esistenti e modifica le righe corrispondenti, registrando gli indirizzi della rete AppleTalk configurati. In questo caso, alla fine del file, troverete la seguente riga:

```
eth0 -phase 2 -net 0-65534 -addr 65280.57
```

Se volete eseguire configurazioni più complesse, troverete degli esempi nel file di configurazione. Per le opzioni supplementari, consultate la manual page di afpd.

Definire il file server – afpd.conf

Il file `afpd.conf` definisce come debba apparire il vostro file server sui computer Mac-OS nel menù di 'Scelta'. Come gli altri file di configurazione, anche questo contiene commenti dettagliati che spiegano le varie opzioni.

Se qui non eseguite alcuna modifica, viene avviato solo il default server e mostrato nella 'Scelta' con i nomi degli host. In questo caso non vi è quindi alcuna necessità di impostare valori, mentre è possibile definire i file server con diversi nomi ed opzioni, per offrire p.e. uno speciale "Guest Server", sul quale è possibile archiviare file sotto forma di "ospiti":

```
"Guest server" -uamlist uams_guest.so
```

Oppure potete definire un server non accessibile agli "ospiti", ma solo agli utenti esistenti sul sistema Linux:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so
```

Questo comportamento viene regolato dall'opzione `uamlist`, a cui segue una lista dei moduli di autentificazione da usare, separata da virgole. Il default consiste nel fatto che tutti i procedimenti sono attivi.

Come standard, un AppleShare-Server mette a disposizione i suoi servizi non solo tramite AppleTalk, ma anche (“incapsulati”) tramite TCP/IP. La default porta è il 548. Se volete che anche i server AppleShare supplementari (sullo stesso computer) usino TCP, dovete attribuire loro determinate porte. Accedere ai servizi tramite TCP/IP permette anche l’accesso al server di reti non-AppleTalk come, p.e., l’Internet.

La sintassi sarebbe:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so -port 12000
```

Il server AppleShare appare poi nella rete con il nome “Font Server”, non permette alcun accesso agli “ospiti” ed è impostato sulla porta 12 000. In questo modo è raggiungibile anche con router TCP/IPD.

Nel file `AppleVolumes.default` (che spiegheremo dettagliatamente più avanti) viene stabilito quali directory (residenti sul server) del rispettivo server AppleShare vengano messe a disposizione come “Volume” della rete (= directory raggiungibili tramite la rete). Con l’opzione `-defaultvol` è possibile stabilire, per un server AppleShare, anche un altro file nel quale vengono eseguite impostazioni divergenti, p.e. (in una riga):

```
"Guest server" -uamlist uams_guest.so -defaultvol
/etc/atalk/AppleVolumes.guest
```

Altre opzioni sono spiegate nel file `afpd.conf`.

Directory e diritti di accesso – AppleVolumes.default

Qui definite quali siano le directory da esportare. I diritti di accesso vengono stabiliti per mezzo dei consueti diritti degli utenti e dei gruppi di Unix.

Tale configurazione avviene nel file `AppleVolumes.default`.

Nota

In parte, qui si è modificata la sintassi: tenetelo presente quando fate l'update da una versione più vecchia a quella attuale; p.e. ora, invece di `access=`, si dice `allow:` (un sintomo caratteristico, sarebbe la visualizzazione – sul client Mac su AppleTalk – delle opzioni invece della denominazione stessa del drive). Poiché ad un update vengono creati nuovi file con l'estensione `.rpmnew`, può darsi che, a causa della sintassi modificata, le vostre vecchie impostazioni non funzionino più.

Vi consigliamo di eseguire un backup dei vostri file di configurazione, di portare dal backup le vecchie impostazioni nei nuovi file e di rinominare quindi i nuovi file. In questo modo, approfittate anche degli attualissimi e dettagliati commenti dei file di configurazione.

Nota

Assieme a `AppleVolumes.default`, possono venire creati altri file come p.e. `AppleVolumes.guest`, utili a determinati tipi di server (con l'uso dell'opzione `-defaultvol` nel file `afpd.conf`; vd. sezione precedente.).

La sintassi è molto semplice:

```
/usr/local/psfonts "PostScript Fonts"
```

significa che la directory Linux `/usr/local/psfonts`, che si trova nella directory root, viene resa disponibile come AppleShare-Volume con il nome "PostScript Fonts".

Le opzioni vengono aggiunte alla riga, separate da uno spazio vuoto. Un'opzione molto utile è la restrizione dei diritti di accesso:

```
/usr/local/psfonts "PostScript Fonts" allow:User1,@gruppe0
```

limita l'accesso al volume "PostScript Fonts" all'utente "User1" e ai componenti del gruppo "gruppo0": naturalmente, questi devono essere noti al server. Allo stesso modo, potete escludere determinati utenti con `deny:User2`

Ricordate che queste limitazioni valgono per l'accesso tramite AppleTalk e non hanno niente a che fare con i diritti dell'utente, se ha la possibilità di fare il login sul server stesso.

Per la raffigurazione delle risorse-fork dei file tipiche di Max OS, Netatalk crea directory `.AppleDouble` nel filesystem di Linux. Con l'opzione `noadouble` potete stabilire che queste directory vengano create solo se sono veramente necessarie. Sintassi:

```
/usr/local/guests "Guests" options:noadouble
```

Le spiegazioni contenute nel file stesso Vi aiuteranno a trovare altre opzioni e possibilità.

Inoltre: in questo file di configurazione trovate anche una tilde (`'~'`). Questa tilde rappresenta la home directory di ogni utente sul server. In questo modo, si può mettere automaticamente a disposizione di ogni utente la sua home directory senza dover indicare esplicitamente ogni singolo utente. Il file-esempio installato contiene già una tilde e, se non modificate il file, Netatalk mette a disposizione la home directory.

Nella home directory di ogni utente registrato, afpd cerca un file `Applevolumes` o `.Applevolumes`. Le impostazioni in questo file completano quelle dei file del server `AppleVolumes.system` e `AppleVolumes.default`, per rendere possibile ulteriori attribuzioni individuali type/creator e per accedere ai file system. Queste impostazioni sono completamenti che impediscono all'utente registrato accessi non autorizzati dal server.

Il file `netatalk.pamd` serve per l'autenticazione tramite PAM (Pluggable Authentication Modules), ma al momento non ci interessa.

Attribuzioni di file – `AppleVolumes.system`

Nel file `AppleVolumes.System` stabilite quali attribuzioni type e creator (tipiche di Mac OS) devono seguire determinate estensioni di file: sono già definiti una serie di valori standard. Se un file viene indicato con un'icona bianca generica, significa che non esiste ancora una impostazione. Se doveste aver problemi ad aprire, sotto Mac OS, un file di testo di un altro sistema (o viceversa), controllate le impostazioni lì contenute.

Configurazione del server della stampante

Nel file `papd.conf` viene messo a disposizione un servizio Laserwriter. La stampante deve già funzionare localmente con l'lpd. Se potete stampare localmente con il comando `lpr file.txt`, avete già fatto un importante primo passo.

Se, su Linux, è configurata una stampante locale, non dovete impostare niente in `papd.conf`, poichè, senza ulteriori indicazioni, gli incarichi di stampa vengono semplicemente inoltrati al daemon della stampante `lpd`. La stampante si fa riconoscere nella rete AppleTalk come Laserwriter. Impostate quindi una stampante nel file di configurazione:

```
Ricezione_stampante:pr=lp:pd=/etc/atalk/kyocera.ppd
```

Questi parametri fanno apparire, nella selezione, la stampante con il nome Ricezione_Stampante. Il corrispondente file di descrizione della stampante si trova generalmente dal produttore. Oppure, prendete il file `Laserwriter` dalla cartella 'Estensioni del sistema'; in questo modo, però, non potete usufruire di tutte le proprietà della stampante.

Inizializzare il server

Il server stesso viene inizializzato con "Init-Skript" allo start del sistema o manualmente con il comando `rcatalk start`. Lo script Init si trova su `/etc/init.d/atalk`.

Il server viene avviato dallo script in sottofondo; occorre circa un minuto, prima che le interfacce AppleTalk siano configurate ed accessibili. Con una richiesta di stato potrete vedere il processo è terminato (lo riconoscerete da `OK` emesso tre volte):

```
terra:~ #  rcatalk status
```

"Checking for service atalk:OKOKOK"

Passate ora ad un Mac su Mac OS. Controllate che Apple Talk sia attivato, selezionate 'File sharing', eseguite un doppio clic su 'Apple share'; nella finestra dovreste ora vedere il nome del vostro server. Eseguitevi un doppio clic e fate il log in. Selezionate il drive e ... voilà, ecco il vostro drive di rete su Mac OS.

Potete collegarvi con i server che funzionano solo con TCP e non con DDP, cliccando nella 'Scelta' su 'Indirizzo IP del server' e registrando l'indirizzo IP corrispondente, eventualmente seguito da due punti e il numero di porta.

Ulteriori informazioni

Per sfruttare tutte le possibilità offerte dal pacchetto `netatalk`, vi consigliamo di leggere la manual page corrispondenti. Come sempre, le troverete con il comando: `rpm -qd netatalk`.

Ancora un avviso: il file `/etc/atalk/netatalk.conf` non viene usato nella nostra versione di netatalk: ignoratelo.

URL di appoggio:

- `http://netatalk.sourceforge.net/`
- `http://www.umich.edu/~rsug/netatalk/`

- http://www.anders.com/projects/netatalk/
- http://cgi.zettabyte.net/fom-serve/netatalk/cache/1.html

E come stanno le cose, viste in senso inverso? Si può accedere ad un drive AppleShare su Linux? La nostra risposta: è meglio di no, dal momento che il pacchetto corrispondente si trova ancora in uno stadio pre-alfa. I più coraggiosi lo trovano all'indirizzo: http://www.panix.com/~dfoster/afpfs/

Internet

Questo capitolo vi mostra come configurare un server proxy Squid. Con questo servizio accelerete l'accesso alle vostre risorse sul world wide web.

Server proxy: Squid 272

Server proxy: Squid

La Proxy cache più diffusa per le piattaforme Linux/UNIX, è Squid. Descriveremo come configurarla, quali sono le esigenze poste al sistema, come deve essere configurato il proprio sistema per poter eseguire un proxying trasparente ed infine come si ottengono statistiche sull'utilità della cache con l'aiuto di programmi come Calamaris e cachemgr o come si filtrano contenuti web con squidgrd.

Cos'è una Proxy-Cache?

Squid funge da Proxy-Cache. Si comporta come un intermediario che riceve richieste da client (in questo caso il browser web) e le inoltra al server-provider competente. Quando gli oggetti richiesti arrivano all'intermediario, questi ne ritiene una copia nella cache del disco rigido.

Il vantaggio si mostra quando più client richiedono lo stesso oggetto: essi possono ora venire serviti direttamente dalla cache del disco rigido, molto più velocemente che dall'Internet. Ciò risparmia molta banda del sistema.

Suggerimento

Squid offre un vasto spettro di proprietà; p.e. la definizione di gerarchie per il proxy server per la distribuzione dei carichi del sistema, designazione di regole di accesso fisse, per tutti i client che vogliono accedere a Proxy, assegnazione o rifiuto dei diritti di accesso su determinate pagine Web con l'aiuto di altre applicazioni o l'emissione delle statistiche delle pagine web maggiormente visitate (p.e. il comportamento di navigazione degli utenti in internet)

Suggerimento

Squid non è un Proxy generico; normalmente fa solo da mediatore fra i collegamenti HTTP. Inoltre appoggia i protocolli FTP, Gopher, SSL e WAIS, ma non altri protocolli internet come Real Audio, News o conferenze video. Squid sostiene il protocollo UDP solo per supportare la comunicazione fra le diverse cache, questo è il motivo per cui non vengono appoggiati nemmeno altri programmi multi media.

Informazioni sulla cache proxy

Squid e la sicurezza

Squid può essere usato insieme ad un firewall per proteggere reti interne da attacchi dall'esterno con l'uso di una cache proxy. Il firewall, fatta eccezione

per Squid rifiuta tutti i servizi esterni e tutte le connessioni al World Wide Web deve essere create attraverso il proxy.

Nel caso di una configurazione firewall con una DMZ (zona demilitarizzata), imposteremmo lì il nostro Proxy: qui è importante che tutti i computer nella DMZ mandino i loro file di protocollo ai computer che si trovano dentro la rete sicura.

Una possibilità per implementare questa proprietà con l'aiuto di un Proxy cosiddetto "trasparente", viene trattata nel sezione 11 a pagina 283.

Diverse cache

Il concetto di cache consiste nel configurare più cache in modo tale che gli oggetti possano venire scambiati fra di esse per ridurre così il carico del sistema ed aumentare la possibilità di trovare un oggetto già esistente nella rete. Questo concetto permette anche la configurazione di gerarchie cache, cosicché una cache è in grado di inoltrare richieste di oggetti a cache della stessa gerarchia, o indurre una cache superiore (nella gerarchia) a scaricare (download) gli oggetti da un'altra cache nella rete locale o direttamente dai file originali.

La scelta della topologia giusta per la gerarchia della cache è molto importante allo scopo di impedire l'aumento del traffico nella rete. In una grande rete, è p.e. possibile configurare un proxy server per ogni sottorete e collegare poi il server Proxy con il Proxy superiore, il quale a sua volta viene nuovamente collegato alla cache proxy dell'ISP.

L'intera comunicazione viene controllata da ICP (ingl. *Internet Cache Protocol*), che è basato sul protocollo UDP. Lo scambio di dati fra le cache avviene tramite HTTP (ingl. *Hyper Text Transmission Protocol*) che si basa su TCP. Per tali collegamenti, dovrebbero però venire utilizzati protocolli più veloci e semplici e che sono in grado di reagire a richieste entro uno o due secondi.

Per trovare il server migliore per gli oggetti desiderati, la cache invia una richiesta ICP a tutti i Proxy della stessa gerarchia. Se l'oggetto è stato trovato, i proxy reagiscono alle richieste con il codice "HIT" tramite risposte ICP; se non è stato trovato, reagiscono con il codice "MISS". Nel caso di più risposte HIT, il server Proxy dà l'incarico ad un server di eseguire il download: questa decisione viene determinata fra l'altro dalla cache che invia la risposta più veloce o dalla cache più vicina. Se non viene inviata alcuna risposta soddisfacente, la richiesta viene inviata alla cache superiore.

Suggerimento

Per evitare la memorizzazione molteplice di oggetti in diverse cache della nostra rete, vengono usati altri protocolli ICP come p.e. CARP (ingl. *Cache Array Routing Protocol*) o HTCP (ingl. *Hyper-Text Cache Protocol*).

Più oggetti si trovano nella nostra rete, più grande è la possibilità di trovare quello cercato.

Suggerimento

La memorizzazione temporanea di oggetti scaricati dall'Internet

Non tutti gli oggetti disponibili nella nostra rete sono statici; molti, come le pagine CGI, i contatori di accesso o i documenti SSL cifrati, vengono generati in maniera dinamica, per una maggiore sicurezza. Per questo motivo, tali oggetti non vengono conservati nella cache, ma modificati ad ogni accesso.

Quanto dovrebbero restare nella cache tutti gli altri oggetti? Per facilitare questa decisione, essi vengono assegnati a tre stadi diversi:

Attraverso header come `Last modified` ("modificato recentemente") o `Expires` ("scade") e la data corrispondente, i server web e proxy si informano sullo stato di un oggetto. Vengono usati anche altri header che per esempio mostrano che un oggetto non deve essere memorizzato temporaneamente.

Gli oggetti nella cache di solito vengono sostituiti a causa di mancanza di spazio di memoria attraverso algoritmi del tipo LRU (ingl. *Last Recently Used*) che sono stati concepiti per sostituire oggetti della cache. Il principio è quello di sostituire innanzitutto gli oggetti meno richiesti.

Requisiti di sistema

Per prima dovrebbe venire definito il carico massimo del sistema: a questo scopo, è importante dare più peso alle punte di carico del sistema, poichè queste possono essere di quattro volte maggiori della media giornaliera. In caso di dubbio, è consigliabile sopravvalutare queste esigenze, ammesso che uno Squid al limite delle sue prestazioni, porti ad una seria perdita della qualità del servizio.

Vi elencheremo ora i diversi requisiti di sistemi in ordine di importanza.

Disco rigido

Per la memorizzazione intermedia, la velocità ha un ruolo molto importante; occupatevi perciò in modo particolare di questo fattore. Nei dischi rigidi, questo parametro è indicato in millesimi di secondo come "tempo casuale di posizionamento". Come regola approssimativa vale: più basso è il valore, più veloce è il disco.

Dimensioni della cache del disco rigido

Le dimensioni della cache del disco rigido dipendono da alcuni fattori. La probabilità di un HIT (l'oggetto desiderato si trova già nella cache) in una cache piccola è molto scarsa, perché questi si riempirà molto velocemente. In questo caso, gli oggetti poco richiesti, vengono sostituiti da nuovi. Se la cache ha però a disposizione `1 GB` e gli utenti hanno bisogno di soli `10 MB` al giorno per navigare in internet, per riempire la cache occorreranno più di 100 giorni.

La dimensione della nostra cache può venire facilmente determinata con la velocità di trasmissione del nostro collegamento. Con un collegamento di `1 MB/sec` il tasso di trasmissione massima è di `125 KB/sec`. Se il traffico completo dei dati arriva nella cache, entro un'ora avremo un totale di `450 MB`. Partendo dal presupposto che il completo traffico dei dati si svolga entro 8 ore di lavoro, in un giorno avremo "raccimolato" `3,6 GB`. Poichè il collegamento non è stato sfruttato fino in fondo, possiamo partire dal presupposto che la quantità di dati che passa attraverso la nostra cache, sia di ca. `2 GB`. Nel nostro esempio, abbiamo bisogno di `2 GB` di memoria per Squid, allo scopo di tenere nella cache i dati di tutte le pagine visitate durante *un* giorno.

Ricapitolando, possiamo dire che Squid tende a leggere dal disco rigido blocchi di dati o a sovrascriverli, di modo che è più importante il tempo che impiega a trovare questi oggetti sul disco rigido, che possedere un disco con un throughput alto.

RAM

La memoria necessaria a Squid dipende dalla quantità degli oggetti che si trovano in cache. Affinchè i dati possano venire richiesti più velocemente, Squid salva anche nella memoria i (ingl. *cache object pointer*) ed i dati più spesso richiesti. La memoria è più veloce di un hard disk di un milione di volte!

Squid mantiene nella memoria anche molti altri dati, come p.e. una tabella con tutti gli indirizzi IP assegnati, una domain name cache esattamente definita, gli oggetti più spesso richiesti, buffer, elenchi dei controlli di accesso, etc.

È molto importante avere sufficiente memoria per un processo Squid; se dovesse venire trasferito sul disco rigido, il rendimento del sistema verrebbe drasticamente ridotto. Per l'amministrazione della memoria della cache, possiamo usare il tool cachemgr.cgi che viene spiegato nella sezione *cachemgr.cgi* a pagina 286 .

CPU

Il programma Squid non ha bisogno di molte CPU. Il carico del processo aumenta solo allo start e durante il controllo del contenuto della cache. L'impiego di un computer multiprocessore non aumenta la prestazione del sistema, a meno che siano in uso solo parti del codice Squid. Per aumentare l'effettività, è consigliabile usare dischi rigidi più veloci o aggiungere memorie.

Sotto `http://www.cache.ja.net/servers/squids.html` troverete alcuni esempi di sistemi configurati, sui quali gira Squid.

Avviare Squid

Lo Squid su SuSE Linux Enterprise Server è già preconfigurato e può essere subito avviato dopo l'installazione. Premessa per un avvio senza complicazioni: la rete deve essere configurata in modo che siano raggiungibili almeno un name server e anche internet. Potrebbe essere problematico, se si utilizza un collegamento con una configurazione DNS dinamica: in questo caso, almeno il name server dovrebbe essere registrato in maniera permanente, poichè Squid non parte se non trova alcun DN in `/etc/resolv.conf`.

Per avviare Squid, inserite (come `root`) nella riga di comando: `rcsquid start`

Al primissimo start, viene prima creata la struttura della directory in `/var/squid/cache`; ciò viene automaticamente eseguito dallo start script `/etc/init.d/squid` e può durare un paio di secondi. Se sulla destra, in verde appare la parola `done`, significa che Squid è stato avviato con successo. Sul sistema locale è possibile collaudare subito la funzionalità di Squid, registrando nel browser (come Proxy) `localhost` e `Port 3128`. Per permettere a tutti l'accesso a Squid e quindi anche ad internet, è sufficiente modificare, nel file di configurazione `/etc/squid.conf`, la formulazione `http_access deny all` in `http_access allow all`. Tenete però presente che, in questo modo, aprite Squid a tutti; è quindi necessario definire le ACL che regolano l'accesso al Proxy. Per maggiori approfondimenti, vd. paragrafo 11 a pagina 280.

Se si sono eseguite modificazioni al file di configurazione `/etc/squid.conf`, si deve indurre Squid a leggerlo di nuovo. Questo avviene con:

```
rcsquid reload
```

Alternativamente, è possibile riavviare Squid:

```
rcsquid restart
```

Importante è anche questo comando:

```
rcsquid status
```

Con esso si può stabilire se il Proxy sta lavorando, e con

```
rcsquid stop
```

si può terminare Squid. Può durare un po', poichè Squid aspetta fino ad un mezzo minuto (Option `shutdown_lifetime` in `/etc/squid.conf`), prima di interrompere i collegamenti con i client e deve anche scrivere i suoi dati sul disco rigido. Terminare Squid con un `kill` o `killall`, può portare alla distruzione della cache. Per riavviare Squid avreste poi bisogno di cancellarla completamente.

Se dopo breve tempo Squid si ferma, nonostante l'avvio sia apparentemente ben riuscito, può essere causa di una registrazione name server errata o della mancanza di un `/etc/resolv.conf`. Squid protocolla nel file `/var/squid/logs/cache.log` la causa di uno start fallito.

Se Squid deve venire avviato automaticamente al boot, nel runlevel editor di YaST2 bisogna attivare Squid per determinati runlevel.

Se disinstallate Squid la cache e i file di log rimangono; di conseguenza, si deve cancellare manualmente la directory `/var/squid`.

Server DNS locale

Configurare un server DNS locale come BIND-8 o BIND-9 è senz'altro ragionevole, anche se non amministra alcun dominio: funge solo da "Caching-only DNS" ed è anche in grado di risolvere, tramite il server dei nomi root, richieste DNS senza bisogno di configurazioni speciali. Se lo si registra nel `/etc/resolv.conf` con l'indirizzo IP `127.0.0.1` per il localhost, allo start Squid trova sempre un server dei nomi valido. La configurazione di un name server è un capitolo a parte e non viene descritta qui; affinchè essa venga eseguita automaticamente, è sufficiente installare ed inizializzare il pacchetto. Il name server del provider deve venire registrato, con il suo indirizzo IP, nel file di configurazione `/etc/named.conf` sotto forwarders. Se esiste un firewall in funzione, anche se si tratta solo di un personal firewall, si deve fare attenzione che vengano ammesse le richieste DNS.

Il file di configurazione /etc/squid.conf

Tutte le impostazioni del proxy server Squid devono venire eseguite nel file `/etc/squid.conf`; per poter inizializzare Squid per la prima volta, non è necessario apportarvi alcuna modifica, ma, in un primo momento, è disdetto l'accesso ai client esterni. Il Proxy è libero per il localhost e, come porta, viene usato di norma il `3128`. Le opzioni sono documentate dettagliatamente e con molti esempi nel file preinstallato `/etc/squid.conf`. Quasi tutte le righe sono hanno all'inizio il segno di commento #, mentre, alla fine della riga, troverete le relative specificazioni. I valori indicati corrispondono quasi sempre ai valori preimpostati, cosicché l'eliminazione del carattere di commento, senza la modificazione del parametro dell'opzione, non ha alcun effetto – con poche eccezioni. È sempre meglio lasciare invariato l'esempio ed inserire l'opzione con il parametro modificato nella riga inferiore. In questo modo, è possibile seguire senza problemi i valori preimpostati e le modificazioni.

Se avete eseguito un'update di una vecchia versione di Squid, è strettamente consigliabile usare il nuovo `/etc/squid.conf` e adottare solo le modificazioni del file originale. Se cercate di continuare ad utilizzare il vecchio `squid.conf`, correte il pericolo che la nuova configurazione non funzioni più, poichè le opzioni vengono continuamente modificate e ne vengono sempre aggiunte delle nuove.

Opzioni generali di configurazione

http_port 3128 La porta sulla quale Squid sta in "ascolto" per quanto concerne le richieste dei client. È preimpostata su `3128`, ma viene usato anche `8080`. Qui è possibile indicare più numeri di porte, divisi da uno spazio.

cache_peer <hostname> <type> <proxy-port> <icp-port> Qui è possibile indicare un Proxy superiore come "parent" (genitore), p.e. se si vuole o deve usare il Proxy del provider. Come `<hostname>` viene registrato il nome o l'indirizzo IP del Proxy da usare e come `<type>` viene registrato `parent`. Per la `<proxy-port>` si digita il numero della porta che l'utente del parent indica anche per l'uso nel browser; nella maggior parte dei casi, si tratta di `8080`. Se non è nota la porta ICP del parent e non se ne è concordato l'uso con il provider, l'`<icp-port>` può venire impostata su `7` o su `0`. Inoltre, dopo il numero della porta si deve anche indicare `default` e `no-query`, per impedire completamente l'uso del protocollo ICP. Dopo di ciò, nei confronti del Proxy del provider, Squid si comporterà come un normale browser.

cache_mem 8 MB Questa registrazione indica il massimo di memoria principale usata da Squid per il Caching. La preimpostazione è di `8 MB`.

cache_dir ufs /var/cache/squid 100 16 256 La registrazione `cache_dir` indica la directory nella quale vengono archiviati tutti gli oggetti sul disco rigido. I numeri posposti indicano lo spazio massimo utilizzabile in `MB` e la quantità di directory nel primo e secondo livello. Il parametro `ufs` dovrebbe rimanere invariato. Nella directory `/var/squid/cache` sono preimpostati `100 MB` di memoria del disco rigido da occupare e vi possono venire create 16 sottodirectory che a loro volta contengono 256 directory. All'indicazione della memoria da utilizzare, si devono lasciare riserve sufficienti; ragionevoli valori fra 50 e al massimo 80% dello spazio disponibile. È bene essere molto prudenti con l'aumento della quantità delle directory, poichè troppe directory possono causare problemi di prestazione. Se esistono più dischi rigidi sui quali distribuire la cache, è possibile registrare il numero di righe `cache_dir` adeguato.

cache_access_log /var/squid/logs/access.log Path per i log file.

cache_log /var/squid/logs/cache.log Path per i log file.

cache_store_log /var/squid/logs/store.log Path per i log file.
Queste registrazioni indicano il path nel quale Squid protocolla tutto ciò che fa. Normalmente, in queste tre registrazioni non è necessario eseguire alcuna modificazione. Se lo Squid viene sottoposto a molto lavoro, può essere consigliabile porre la cache e i log file su diversi dischi rigidi.

emulate_httpd_log off Se si cambia la registrazione in `on`, si ricevono log file leggibili. Alcuni programmi di analisi però non riescono a lavorare con essi.

client_netmask 255.255.255.255 Con questa registrazione è possibile mascherare nei log file gli indirizzi IP protocollati per nascondere l'identità del client. Se qui viene registrato `255.255.255.0`, l'ultimo posto dell'indirizzo IP viene impostato sullo zero.

ftp_user Squid@do.main Specificare qui la password che Squid debba usare per i login anonimi su FTP. Alternativamente, potete indicare anche un indirizzo di e-mail del vostro dominio, dal momento che alcuni server FTP ne verificano la validità.

cache_mgr webmaster Si tratta di un indirizzo e-mail al quale Squid invia una notizia nel caso di crollo. È preimpostato `webmaster`.

logfile_rotate 0 Se si chiama `squid -k rotate`, Squid è in grado di far ruotare i file log memorizzati: i file vengono numerati in relazione alla loro quantità e, dopo aver raggiunto il valore indicato, il file più vecchio viene sovrascritto. Di norma, questo valore è impostato su `0`, perché in SuSE Linux Enterprise Server l'archiviazione e cancellazione di file log vengono eseguite da un proprio cron job la cui configurazione si trova nel file `/etc/logrotate/syslog`. Il periodo di tempo dopo il quale i file vengono eliminati viene fissato nel file `/etc/sysconfig/aaa_base`, con la riga `MAX_DAYS_FOR_LOG_FILES`.

append_domain <domain> Con `append_domain` si può indicare quale domain venga automaticamente aggiunto, se non se ne è indicato alcuno. Nella maggior parte dei casi, qui viene indicato il proprio domain, dopo di ciò, per arrivare al proprio web server, è sufficiente indicare `www` nel browser.

forwarded_for on Se si imposta questa registrazione su `off`, Squid toglie dalle richieste HTTP, l'indirizzo IP o il nome del sistema del client.

negative_ttl 5 minutes; negative_dns_ttl 5 minutes Normalmente non è necessario modificare questi valori. Se si ha però un collegamento a selezione, può succedere che per un po' internet non sia raggiungibile: Squid si ricorda delle richieste inutili e si rifiuta di ripeterle, benchè il collegamento con internet sia nuovamente attivo. In un tale caso, si possono modificare i `minutes` in `seconds` cosicchè, dopo pochi secondi dalla selezione, anche un `Reload` nel browser porta al successo.

never_direct allow <acl_name> Se si vuole evitare che Squid esiga le richieste direttamente da Internet, con la registrazione sopra citata, si può costringere l'impiego di un altro Proxy, che deve prima essere stato registrato sotto `cache_peer`. Se come `<acl_name>` si indica `all`, si ottiene che tutte le richieste vengano inoltrate direttamente al `parent`. Ciò può essere necessario se p.e. si utilizza un provider che prescrive l'uso del suo Proxy o se il firewall non fa passare alcun accesso diretto ad Internet.

Opzioni per il controllo dell'accesso

Squid offre un sistema raffinato per il controllo dell'accesso al Proxy: con le ACL, è molto semplice configurarlo in diversi modi. Si tratta di elenchi di regole che vengono elaborate una dopo l'altra. Prima di poter essere usate, le ACL devono venire definite. Alcune ACL standard come `all` e `localhost`

lo sono già. Di per sé, la definizione di una ACL non ha ancora nessuna conseguenza: solo quando viene usata, p.e. in collegamento con `http_access`, vengono utilizzate le regole stabilite.

acl <acl_name> <type> <data> Per una definizione, una ACL ha bisogno di almeno tre indicazioni: il nome `<acl_name>` può venire scelto liberamente. Per `<type>` è possibile scegliere fra una quantità di possibilità diverse che potrete vedere nella sezione `ACCESS CONTROLS` in `/etc/squid.conf`. I `<data>` (dati) da indicare, dipendono dal tipo corrispondente di ACL e possono venire letti anche da un file, p.e. con nome di computer, indirizzo IP o URL. Eccovi qui di seguito alcuni semplici esempi:

```
acl i-miei-surfer srcdomain .meine-domain.com
acl insegnante src 192.168.1.0/255.255.255.0
acl studenti src 192.168.7.0-192.168.9.0/255.255.255.0
acl mezzogiorno time MTWHF 12:00-15:00
```

http_access allow <acl_name> Con `http_access` viene stabilito chi possa usare il Proxy e a cosa possa accedere su internet: per questo, devono venire indicate ACL che con `deny` o `allow` blocchino o liberino l'accesso – `localhost` e `all` sono già stati spiegati sopra. Qui è possibile creare una lista con parecchie registrazioni `http_access` che vengono elaborate da sopra a sotto; a seconda della registrazione che può venire utilizzata per prima, viene liberato o bloccato l'accesso all'URL richiesto. La registrazione `http_access deny all` dovrebbe sempre essere all'ultimo posto. Nel seguente esempio, `localhost`, il computer locale, ha libero accesso su tutto, mentre per tutti gli altri è bloccato.

```
http_access allow localhost
http_access deny all
```

Ancora un esempio, nel quale nel quale vengono usati le ACL definite prima: il gruppo `insegnante` ha sempre accesso ad Internet, mentre che il gruppo `studenti` vi può navigare solo da lunedì a venerdì e qui solo a mezzogiorno.

```
http_access deny localhost
http_access allow insegnante
http_access allow studenti mezzogiorno
http_access deny all
```

Per motivi di maggior chiarezza, la lista con le proprie registrazioni `http_access`, dovrebbe venire inserita solo nello spazio adeguato in `/etc/squid.conf`. Cioè fra il testo

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

ed il successivo

```
http_access deny all
```

redirect_program /usr/bin/squidGuard Con questa opzione, è possibile indicare un "redirector", come, p.e., SquidGuard, che sia in grado di bloccare URL non desiderati. In collegamento con l'autenticazione Proxy e le ACL adeguate, è possibile regolare molto specificatamente, l'accesso di diversi gruppi di utenti all'Internet. SquidGuard è un pacchetto a sé stante che viene installato e configurato separatemante.

authenticate_program /usr/sbin/pam_auth Se si desidera che gli utenti si identifichino al Proxy, si può indicare qui un programma adeguato, p.e. pam_auth. All'uso di pam_auth, al suo primo accesso, l'utente riceve una finestra di log in nella quale deve inserire l'user ID e la password: oltre a ciò è necessario anche una ACL affinchè possano navigare solo i client con il login valido:

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Quel `REQUIRED` dopo `proxy_auth` può anche essere sostituito con una lista di username autorizzati o un path relativo ad una lista del genere.

ident_lookup_access allow <acl_name> In questo modo, è possibile far eseguire una richiesta di Ident su tutti i client definiti con l'ACL, allo scopo di accertare l'identità del rispettivo utente. Se per `<acl_name>` si inserisce `all`, questo accertamento viene eseguito per tutti i client. A questo scopo, sui client deve correre un Ident-daemon; per Linux, si può installare a questo proposito il pacchetto pidentd, per Windows esiste un software libero che può venire procurato dall'internet. Affinchè possano venire ammessi solo i client con Ident look up valido, deve venire definita una relativa ACL:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Anche qui `REQUIRED` può venire sostituito da un elenco di user ID permessi. L'uso di `Ident` può rallentare notevolmente l'accesso, poichè gli Ident lookup vengono ripetuti per ogni richiesta.

Configurazione del proxy trasparente

Normalmente con i proxy server si lavora come segue: il browser web invia richieste ad una determinata porta nel proxy server e il Proxy mette a disposizione gli oggetti richiesti, sia che siano nella cache o no. All'interno di una rete vera possono subentrare diverse situazioni:

- per ragioni di sicurezza è bene che tutti i client usino un Proxy per navigare in internet.
- È necessario che tutti i client utilizzino un Proxy, sia che ne siano consapevoli o no.
- Per le reti più grandi che utilizzano già un Proxy, è possibile memorizzare le configurazioni modificate dei singoli computer, se nel sistema sono emersi dei cambiamenti.

In ognuno di questi casi, può venire impiegato un Proxy trasparente. Il principio è molto semplice: il Proxy prende le richieste del browser web e le elabora, cosicchè il browser web riceve le pagine richieste senza sapere da dove vengono. Tutto il processo viene eseguito in modo trasparente; da qui il nome del procedimento.

Opzioni di configurazione in /etc/squid.conf

Nel file `/etc/squid.conf` devono essere abilitate le seguenti opzioni per avere un Proxy trasparente:

- httpd_accel_host virtual
- httpd_accel_port 80 # Porta sulla quale si trova il vero server HTTP.
- httpd_accel_with_proxy on
- httpd_accel_uses_host_header on

Configurazione del firewall con SuSEfirewall2

Ora, con l'aiuto di una regola di inoltro per la porta, dobbiamo inoltrare tutte le richieste in arrivo attraverso il firewall.

A questo scopo, viene usato un tool proprio di SuSE: SuSEfirewall2. Il suo file di configurazione si trova nel file `/etc/sysconfig/scripts/SuSEfirewall2-custom`. Il file di configurazione è composto da registrazioni ben documentate. Anche se vogliamo configurare solo un Proxy trasparente, dobbiamo configurare alcune opzioni firewall, p.es.:

- device punta su Internet: FW_DEV_WORLD="eth1"
- device punta sulla rete: FW_DEV_INT="eth0"

Sono delle reti inaffidabili come Internet ad accedere a porte e servizi (vd. `/etc/exports`) nel firewall. Nel seguente esempio, offriamo solo servizi web in uscita:

FW_SERVICES_EXTERNAL_TCP=www

Reti sicure, come pure TCP e UDO, accedono a porte/servizi (vd. `/etc/exports`) nel firewall.

FW_SERVICES_INTERNAL_TCP=domain www 3128

FW_SERVICES_INTERNAL_UDP=domain

Accediamo ai servizi web e a Squid (la cui porta standard è 3128).

Il servizio sopra descritto "Domain" sta per DNS o Domain Name Server: è usuale utilizzarlo. Diversamente lo togliamo dalla registrazione (vedi sopra) e impostiamo l'opzione su no:

L'opzione più importante è la cifra 15:

```
FW_SERVICE_DNS="yes"
```

```
#
# 15.)
# Quale accesso ai singoli servizi deve venire deviato ad una porta
# locale sul computer firewall?
#
# Con ciò, tutti gli utenti esterni possono venire costretti a
# navigare tramite lo Squid Proxy oppure è possibile deviare in
# maniera trasparente, il traffico web entrante ad un server web
# sicuro.
#
```

```
# Scelta: non eseguire alcuna registrazione o usare la sintassi
# delle regole di deviazione spiegata qui di seguito e divisa da
# uno spazio vuoto. Una regola di deviazione consiste in 1) Source
# IP/rete, 2) meta IP/rete, 3) porta meta originale e 4) porta locale
# alla quale deve venire deviato il sistema e separato
# da virgole, p.e. "10.0.0.0/8,0/0,80,3128
# 0/0,172.20.1.1,80,8080"
#
```

file 48: *Opzione 15 della configurazione del firewall*

Nel commento sopra riportato, viene mostrata la sintassi da rispettare. Prima accedono gli indirizzi IP e la scheda rete delle "reti interne" al firewall di Proxy: quindi gli indirizzi IP e le maschere rete ai quali i client inviano le richieste. Nel caso dei browser, stabiliamo le reti 0/0; si tratta di una wildcard e significa "dappertutto". Segue la porta "originale", alla quale sono state spedite queste richieste, e, infine, segue la porta a cui sono state "deviate" le richieste.

Dal momento che Squid supporta più protocolli del semplice HTTP, potete deviare al proxy anche le richieste da altre porte, come FTP (Port 21), HTTPS o SSL (Porta 443).

Concretamente, i servizi web (Port `80`) vengono deviati alla proxy port (in questo caso: `3128`). Qualora vogliate aggiungere altre reti o servizi, dovrete separarli con uno spazio nella riga corrispondente.

FW_REDIRECT_TCP=192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128

FW_REDIRECT_UDP=192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128

Per inizializzare il firewall e la nuova configurazione, dobbiamo editare una registrazione nel file `/etc/sysconfig/SuSEfirewall2`. La registrazione START_FW deve venire impostata su yes:

Per controllare se tutte le porte sono state configurate correttamente, si può eseguire un port scan sul computer – da un qualsiasi computer al di fuori della nostra rete. Solo la porta di servizio web (80) dovrebbe essere aperta. Il port scan passa attraverso e per `nmap`:

```
nmap -O IP_address
```

Squid e altri programmi

In questa sezione vi mostriamo come integrare altre applicazioni con Squid. cachemgr.cgi rende possibile all'amministratore del sistema, di controllare lo spazio necessario per la memorizzazione intermedia di oggetti. Squidgrd filtra pagine web e calamaris è un generatore di prospetti per Squid.

cachemgr.cgi

Il cache manager (cachemgr.cgi) è un programma di aiuto CGI, per l'emissione di statistiche sulla memoria necessaria dal processo Squid in corso. Al contrario dall'esecuzione di protocolli, la cosa facilita l'amministrazione della cache e la visualizzazione di statistiche.

Configurare

Per prima cosa, sul nostro sistema abbiamo bisogno di un server web funzionante. Per sapere se Apache è già in funzione, dobbiamo inserire come utente `root`: `rcapache status`

Se appare una comunicazione come la seguente:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

vuol dire che Apache gira sul nostro computer: se questo non è il caso dobbiamo immettere: `rcapache start`

Potremo farlo funzionare con le impostazioni standard di SuSE Linux.

Per ultimo, dobbiamo copiare il file `cachemgr.cgi` nella directory `cgi-bin` di Apache:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi
/srv/www/cgi-bin
```

Il cache manager ACL in /etc/squid.conf

Le seguenti impostazioni standard sono necessarie per il cache manager:

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Dovrebbero essere contenute le seguenti regole:

```
http_access allow manager localhost
http_access deny manager
```

La prima ACL è la più importante, poichè il cache manager cerca di comunicare con lo Squid tramite il protocollo cach_object.

Le seguenti regole partono dal presupposto che il server web e Squid girino sullo stesso computer. La comunicazione fra il cache manager e Squid origina nel server web e non nel browser. Se quindi il server web si trova su un altro computer, dobbiamo aggiungere appositamente una ACL nel seguente file esempio 49

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # IP server web
```

file 49: *Regole di accesso*

Inoltre servono le seguenti regole dal file 50.

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

file 50: *Regole di accesso*

Se vogliamo accedere a più opzioni (p.e. chiudere la cache da remoto o visualizzare altre informazioni tramite la cache), possiamo anche configurare una password per il manager. Dobbiamo configurare con una password per il manager, la registrazione cachemgr_passwd e la lista delle opzioni che vogliamo farci visualizzare. Questa lista appare in `/etc/squid.conf` come parte dei commenti delle registrazioni.

Ad ogni modifica del file di configurazione, bisogna riavviare Squid con il comando `-k reconfigure.`

Visualizzare le statistiche

Andate alla pagina web relativa, p.e.:
`http://webserver.example.org/cgi-bin/cachemgr.cgi`

Premete su 'continue' e fatevi mostrare le diverse statistiche. Nelle FAQ di Squid, `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html` troverete ulteriori informazioni sulle singole registrazioni che vengono emesse dal cache manager.

SquidGuard

Questo capitolo, vuole solo essere una introduzione alla configurazione di SquidGuard e darvi un paio di consigli sul suo impiego. Troverete informazioni più dettagliate sulle pagine web di SquidGuard: `http://www.squidguard.org`.

SquidGuard è un filtro libero (GPL), flessibile e velocissimo, che si occupa della deviazione e inoltre un "Access-Controller-PlugIn" per Squid: permette, per una Squid cache, la definizione di una quantità di regole di accesso

con diversi limiti per diversi gruppi di utenti. Per la deviazione, SquidGuard utilizza l'interfaccia standard di Squid.

squidGuard può anche venire utilizzato per:

- Limitazione dell'accesso Internet per alcuni utenti, a determinati web server e/o URLs accettati/conoscuiti.
- Rifiuto di accesso per alcuni utenti a determinati server web e/o URL.
- Rifiuto di accesso per alcuni utenti a URL contenenti determinate espressioni o termini.
- Deviare URL bloccati a una pagina info "intelligente" e che si basa su CGI.
- Deviazione degli utenti non registrati ad un modulo di registrazione.
- Deviare banner su un GIF vuoto.
- Differenti regole di accesso, dipendenti dall'orario, giorno, data, etc.
- Differenti regole per i singoli gruppi di utenti.

Né con squidGuard, né con Squid è possibile:

- filtrare/censurare/editare testo entro i documenti
- filtrare/censurare/editare linguaggi script come JavaScript o VBscript che si trovano in HTML.

L'uso di SquidGuard

Installate il pacchetto `squidgrd`. Editate il file di configurazione `/etc/squidguard.conf`. Sotto `http://www.squidguard.org/config/` troverete numerosi esempi di configurazione. Più avanti potrete "sperimentare" con configurazioni più complicate.

Il prossimo passo, consiste nel creare una pagina dummy "accesso rifiutato" o, se il client richiede una pagina web proibita, creare una pagina CGI più o meno intelligente per deviare Squid. Anche qui vi consigliamo l'uso di Apache.

Ora dobbiamo comunicare a Squid di impiegare SquidGuard. A questo scopo, usiamo nel file `/etc/squid.conf` le seguenti registrazioni:

```
redirect_program /usr/bin/squidGuard
```

Un'altra opzione di nome redirect_children configura la quantità dei diversi "redirect" – processi di deviazione, in questo caso SquidGuard – in corso sul computer. SquidGuard è abbastanza veloce per elaborare una quantità di richieste (è veramente veloce: 100.000 richieste in 10 secondi su un Pentium di 500MHz con 5900 domini, 7880 URLs, in totale 13780). Perciò non consigliamo di stabilire più di 4 processi, poichè l'attribuzione di questi processi consuma inutilmente molta memoria: redirect_children 4

Per ultimo, inviate a Squid un segnale HUP, affinchè venga letta la nuova configurazione

```
squid -k reconfigure
```

Ore potete provare le vostre impostazioni su un browser.

Creare comunicati di cache con Calamaris

Calamaris è uno script Perl che viene usato per creare rapporti di attività della cache in formato ASCII o HTML. Lavora con file di protocolli di accesso propri di Squid. La home page di Calamaris si trova sotto `http://Calamaris.Cord.de/`.

Il programma è semplice da usare: fate il login come `root` ed inserite quanto segue:

```
cat access.log.files | calamaris [options] > reportfile
```

Alla concatenazione di più file di protocollo, è importante l'osservazione della sequenza cronologica, ovvero prima i file più vecchi.

Le diverse opzioni:

-a viene normalmente usate per l'emissione di tutti i rapporti disponibili; con

-w si ottiene un rapporto HTML e con

-l una notizia o un logo nell'header del rapporto.

Nella manual page di calamaris, `man calamaris` troverete altre informazioni sulle diverse opzioni.

Un esempio comune:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \
 >/usr/local/httpd/htdocs/Squid/squidreport.html
```

Il rapporto viene archiviato nella directory del web server. E di nuovo è necessario Apache per poter mostrare i rapporti!

Un altro strumento potente per la creazione di rapporti di cache è SARG (Squid Analysis Report Generator), che troverete nella serie n. Per maggiori informazioni a riguardo, consultate la pagina Internet: http://web.onda.com.br/orso/

Altre informazioni su Squid

Visitate la home page di Squid: http://www.squid-cache.org/. Qui troverete la Squid User Guide e una vasta raccolta di FAQs su Squid.

Il mini HOWTO per un Proxy trasparente è nel pacchetto howtoen, sotto /usr/share/doc/howto/en/mini/TransparentProxy.gz

Inoltre esistono liste mailing per Squid sotto:
squid-users@squid-cache.org.

L'archivio relativo si trova sotto:
http://www.squid-cache.org/mail-archive/squid-users/

Reti sicure

Masquerading, Firewall, Kerberos e ssh sono quattro i quattro pilastri di una rete sicura. In questo capitolo verranno illustrati i principi basilari dei quattro tool e verrà spiegato dettagliatamente il modo di usarli.

Masquerading e Firewall 292
SSH – secure shell, l'alternativa sicura 297
Autenticazione della rete — Kerberos 303
Installare e amministrare Kerberos 310

Masquerading e Firewall

Grazie alle sue spiccate capacità di rete, Linux viene sempre più spesso utilizzato come router per linee commutate e non. Qui la definizione "router" si riferisce ad un computer con più di un'interfaccia di rete ed in grado di inoltrare ai suoi rispettivi partner (spesso chiamati gateway) i pacchetti che non sono destinati ad una delle proprie interfacce di rete. Con i filtri dei pacchetti presenti nel kernel di Linux è possibile controllare esattamente quali pacchetti della trasmissione di dati possano passare e quali no.

Per determinare i precisi criteri di filtraggio per questo filtro di pacchetti, l'amministratore deve avere una certa esperienza. Per gli utenti meno esperti, SuSE Linux contiene un pacchetto a sè stantepacchetto `SuSEfirewall2` inteso a facilitare l'impostazione di queste regole.

La configurazione di SuSEfirewall è molto flessibile ed perciò adatta anche alla creazione di strutture più complesse di filtri di pacchetti.

Questo filtro di pacchetti permette di usare un computer Linux - tramite masquerading - come router per collegare una rete interna con un solo indirizzo IP visibile dall'esterno. Il mascheramento viene anche realizzato in base alle regole di un filtro di pacchetti.

Attenzione

I procedimenti qui presentati sono standardizzati e generalmente funzionano: non possiamo tuttavia garantire che non si sia infiltrato un qualche erroretto in questo manuale o altrove. Se i cracker riescono ad entrare nel Vostro sistema, nonostante abbiate fatto tutto a puntino, non datene la colpa agli autori. Anche se non doveste ricevere una risposta diretta, siate pur certi che Vi saremo grati per ogni Vostra critica o suggerimento e provvederemo immediatamente a fare ammenda

Attenzione

I principi del masquerading

Masquerading è la versione Linux di NAT; NAT significa Network Address Translation, cioè "traduzione di indirizzi rete". Il principio di NAT non è particolarmente complicato: il vostro router ha più di un'interfaccia di rete, normalmente una scheda rete e una interfaccia a parte per l'Internet (p.e. un'interfaccia ISDN). Una di queste interfacce vi collegherà con l'esterno, una o più delle altre interfacce collegheranno il vostro computer agli altri computer

nella vostra rete. Facciamo ora un esempio e ci colleghiamo via ISDN con l'esterno, con l'interfaccia rete esterna `ippp0`. Nella vostra rete locale avete collegato più computer con la scheda rete del router Linux la quale, nel nostro esempio, si chiamerà `eth0`. Gli host nella rete dovrebbero essere configurati in modo da inviare i pacchetti destinati all'esterno a questo gateway.

Nota

Quando configurate la vostra rete, fate attenzione alla concordanza degli indirizzi broadcast e delle maschere rete!

Nota

Se uno dei computer nella vostra rete invia ora un pacchetto in Internet, il pacchetto arriva al vostro router di default. Il router deve essere configurato in modo da inoltrare i pacchetti. Per ragioni di sicurezza, ciò non viene eseguito dall'installazione di SuSE Linux! Modificate la variabile `IP_FORWARD` che si trova nel file `/etc/sysconfig/network/options` in `IP_FORWARD=yes`. Dopo il reboot o con il comando: `echo 1 > /proc/sys/net/ipv4/ip_forward` viene attivato l'inoltro.

Il router vede solo l'indirizzo IP visibile dall'esterno, p.e. l'indirizzo IP dell'interfaccia ISDN connessa. L'indirizzo origine dei pacchetti trasmessi deve essere sostituito dall'indirizzo del router per consentire il reply. Il computer meta del collegamento conosce solo il vostro router, non però il computer mittente nella vostra rete interna, nascosto dietro il vostro router. Da qui il termine "masquerading"(mascheramento).

Il router, quale destinazione di una pacchetto risposta, deve identificare i pacchetti in entrata, modificare l'indirizzo di destinazione in base al ricevente e inoltrarlo all'host nella rete locale. Questo riconoscimento di pacchetti appartenenti a collegamenti creati dal router tramite masquerading avviene con l'aiuto di una tabella depositata direttamente nel kernel del vostro router per il periodo di tempo in cui i rispettivi collegamenti sono attivi: questa tabella può venire esaminata dal superutente (`root`) con i comandi `ipchains` e `iptables`. Per avere indicazioni più precise, consultate la rispettiva documentazione su questi comandi. Per l'identificazione di singoli collegamenti masquerade, sono importanti, oltre all'indirizzo mittente e ricevente, anche il numero della porta ed i protocolli interessati. In questo modo, il Vostro router è in grado di "nascondere" contemporaneamente migliaia di collegamenti per ognuno dei vostri computer locali.

Poichè il percorso dei pacchetti entranti dipende dalla tabella di masquerading, non ci sono possibilità di aprire un collegamento dall'esterno all'interno: questo collegamento non è previsto nella tabella. Nella tabella, ogni collegamento effettuato ha un stato ben determinato, di modo che i relativi

parametri nella tabella non possano venire utilizzati da un secondo collegamento. Di conseguenza, subentrano difficoltà con alcune applicazioni: per esempio ICQ, cucme, IRC (DCC, CTCP), Quake e FTP (nel modo port). Netscape, il programma FTP standard e tanti altri utilizzano il modo PASV che con filtri di pacchetti e masquerading causa meno difficoltà.

Basi del firewall

"Firewall" è probabilmente una delle definizioni più diffuse per descrivere un meccanismo che collega fra loro due reti e che provvede ad un traffico di dati monitorizzato. Esistono diversi tipi di firewall che si distinguono principalmente a livello logico-astratto della verifica e la regolamentazione del traffico dei dati. Per essere più precisi, il metodo che Vi presentiamo qui dovrebbe chiamarsi "filtro di pacchetti". Come ogni altro tipo di firewall, un filtro di pacchetti da solo non garantisce una protezione completa contro ogni rischio di sicurezza. Un filtro di pacchetti regola un transito sulla base di norme i cui criteri sono protocolli, porte ed indirizzi IP. In questo modo, siete in grado di intercettare quei pacchetti che, sulla base del loro indirizzo, non dovrebbero trovarsi nella vostra rete. È per esempio consigliabile intercettare quei pacchetti che utilizzano il servizio telnet sul port 23 del vostro computer. Se però volete permettere l'accesso al vostro web server, dovete attivare la porta corrispondente. Il contenuto di questi pacchetti non viene controllato finché sono indirizzati in modo corretto (p.e. hanno come meta il vostro server web). Il pacchetto potrebbe quindi attaccare il vostro server CGI, senza esser bloccato dal filtro.

Una struttura più efficace, anche se più complessa, potrebbe essere anche caratterizzata da una combinazione di diversi sistemi, come, p.e., la combinazione di un filtro di pacchetti ed un'applicazione gateway/proxy. Il filtro di pacchetti respinge quei pacchetti che non sono indirizzati al port attivato e lascia passare solo i pacchetti per un application gateway. Questo gateway o proxy finge di essere l'interlocutore del server che si vuole collegare con noi. Da questo punto di vista, un tale proxy può essere considerato una macchina di masquerading a livello del protocollo della rispettiva applicazione. Un esempio per un tale proxy, è Squid, un server proxy http, la cui raggiungibilità va configurata nel vostro browser, affinché le richieste di pagine HTML vengano replicate dalla memoria del proxy, anzicché dall'Internet. La SuSE proxy suite (il pacchetto proxy-suite), contiene un server proxy per il protocollo ftp.

In seguito, vogliamo concentrarci sul filtro di pacchetti di SuSE Linux. Per ulteriori informazioni e link consultate l'HOWTO del firewall contenuto nel pacchetto `howtoen`. Se questo pacchetto è stato installato, può venire letto

con il comando `less /usr/share/doc/howto/en/Firewall-HOWTO.gz`.

SuSEfirewall2

Configurare il SuSEfirewall2 è più complesso e richede più esperienza. Sotto `/usr/share/doc/packages/SuSEfirewall2` trovate la documentazione per il SuSEfirewall2.

La configurazione di SuSEfirewall2 viene salvata nel file `/etc/sysconfig/SuSEfirewall2`. Il firewall si lascia configurare con YaST2 ('Sicurezza' → 'Firewall'). Segue una guida alla configurazione passo per passo. In ogni punto, viene indicato se si tratti di masquerading o firewall. Nel file di configurazione si parla anche di una DMZ ("Zona demilitarizzata"); ma questo non è il tema del nostro capitolo.

Se avete veramente bisogno soltanto di masquerading, compilate solo le righe contrassegnate con *Masquerading*

- Inizializzate il SuSEfirewall2 per il vostro runlevel (probabilmente 3 o 5) con l' editor runlevel di YaST2. Così create dei link simbolici per gli script SuSEfirewall2_* nelle directory `/etc/init.d/rc?.d/`.
- FW_DEV_WORLD (Firewall, Masquerading): Per esempio `eth0`, il dispositivo che punta nell'Internet. Nel caso di ISDN è per esempio `ippp0`.
- FW_DEV_INT (Firewall, Masquerading): il device che punta all'interno, nella rete "privata". Se non esiste alcuna rete interna lasciate vuota quest'area.
- FW_ROUTE (Firewall, Masquerading): se avete bisogno di masquerading, rispondete `yes`. I vostri computer interni non sono visibili dall'esterno, dal momento che hanno indirizzi di rete privati (p.e. `192.168.x.x`) che non possono essere indirizzati ("routed") su Internet.

  Con un firewall senza masquerading selezionate qui `yes`, solo se volete permettere l'accesso alla rete interna. Per fare questo i computer interni devono avere indirizzi IP assegnati ufficialmente. Di solito però, *non* dovreste consentire un accesso ai vostri computer dall'esterno!
- FW_MASQUERADE (Masquerading): se avete bisogno del masquerading, immettete `yes`. Tenete presente che è più sicuro se i computer della rete interna accedono a Internet tramite il server proxy.

- FW_MASQ_NETS (Masquerading): indicate qui il computer e/o la rete da mascherare. Dividete le singole impostazioni con spazi vuoti. Esempio: FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
- FW_PROTECT_FROM_INTERNAL (Firewall): immettete qui `yes`, se volete proteggere il firewall anche da attacchi dalla rete interna. In questo caso, dovrete esplicitamente attivare i servizi disponibili per la rete interna. Vedi anche FW_SERVICES_INTERNAL_TCP e FW_SERVICES_INTERNAL_UDP.
- FW_AUTOPROTECT_GLOBAL_SERVICES (Firewall): lasciare di solito su `yes`.
- FW_SERVICES_EXTERNAL_TCP (Firewall): registrate qui i servizi a cui si deve accedere; per esempio `"www smtp ftp domain 443"` – per il computer "domestico" che non deve offrire alcun servizio, non inserite niente.
- FW_SERVICES_EXTERNAL_UDP (Firewall): lasciate libero questo campo, a meno che non stiate usando un nameserver a cui si deve accedere dall'esterno. Altrimenti inserite qui le porte necessarie.
- FW_SERVICES_INTERNAL_TCP (Firewall): qui trovate i servizi disponibili per la rete interna. Le indicazioni sono analoghe a quelle in FW_SERVICES_EXTERNAL_TCP, si riferiscono però qui alla rete *interna*.
- FW_SERVICES_INTERNAL_UDP (Firewall): Vedi sopra.
- FW_TRUSTED_NETS (Firewall): qui registrate quei computer di cui potete *veramente* fidarvi ("Trusted Hosts"). Tenete però a mente che anche questi computer devono venire protetti da intrusioni. Esempio: `"172.20.0.0/16 172.30.4.2"` significa che tutti i computer, il cui indirizzo IP comincia con `172.20.x.x`, come pure il computer con l'indirizzo IP `172.30.4.2` sono abilitati a passare il firewall.
- FW_SERVICES_TRUSTED_TCP (Firewall): qui potete stabilire gli indirizzi port TCP, che possono venire usati dai "Trusted Hosts". Registrate p.e. `1:65535` se i computer affidabili possono accedere a tutti i servizi. Normalmente, dovrebbe essere sufficiente impostare `ssh` come servizio.
- FW_SERVICES_TRUSTED_UDP (Firewall): come sopra, solo riferito a UDP.
- FW_ALLOW_INCOMING_HIGHPORTS_TCP (Firewall): e volete lavorare con un FTP normale (attivo), digitate qui `ftp-data`.

- FW_ALLOW_INCOMING_HIGHPORTS_UDP (Firewall): inserite `dns` per poter usare i nameserver registrati su `/etc/resolv.conf`. Con `yes` attivate tutti i numeri di port alti.
- FW_SERVICE_DNS (Firewall): se lavorate con un nameserver che deve essere accessibile dall'esterno, digitate `yes`; contemporaneamente, su FW_TCP_SERVICES_* deve essere attivata la porta 53.
- FW_SERVICE_DHCLIENT (Firewall): se usate dhclient per ricevere il Vostro indirizzo IP, impostate `yes`.
- FW_LOG_*: indicate qui cosa volete protocollare. Per l'uso corrente basta `yes` in FW_LOG_DENY_CRIT.
- FW_STOP_KEEP_ROUTING_STATE (Firewall): se vi collegate ad Internet tramite diald o ISDN (dial on demand), impostate qui `yes`.

La configurazione così è conclusa. Non dimenticate di testare il firewall (per esempio `telnet` dall'esterno); su `/var/log/messages` dovrebbe apparire più o meno quanto segue:

```
Feb  7 01:54:14 www kernel: Paket log: input DENY eth0
PROTO=6 129.27.43.9:1427 195.58.178.210:23 L=60 S=0x00
I=36981 F=0x4000 T=59 SYN (#119)
```

SSH – secure shell, l'alternativa sicura

Nell'era del networking l'accesso a sistemi remoti diventa sempre più semplice e comune. Al centro di questo processo sta l'autenticazione dell'utente.

Dovrebbe ormai essere ovvio per tutti gli utenti che il proprio nome di utente e la propria password non debbano essere condivisi con nessuno. Questo principio è ormai compreso anche in tutti gli accordi di collaborazione tra aziende, centri informatici o gestori di servizi di comunicazione.

Eppure, la stragrande maggioranza dei processi di autenticazione e di trasmissione dei dati avvengono ancora in forma non cifrata: pensate solo alla posta elettronica che ricevete attraverso il vostro Post Office Protocol (POP) o a quando vi immettete in un sistema remoto tramite telnet. Il che vuol dire che tutti quei dati e quelle informazioni che si considerano confidenziali (il contenuto di una lettera, una conversazione con talk, ecc.) circolano senza

alcun tipo di protezione nella rete. Ciò non rappresenta solo un rischio per la privacy dell'utente, ma espone la comunicazione a potenziali abusi. Queste lacune vengono volentieri usate per attaccare altri sistemi o persino per appropriarsi dei diritti di amministrazione o di root di questi sistemi.

Ogni dispositivo coinvolto nell'inoltro dei dati o impiegato nella stessa rete locale, come firewall, router, switch, mail server, workstation, ecc. è in grado di accedere ai dati stessi. Da un punto di vista legislativo, è illecito appropriarsi di dati altrui. In pratica, però, è difficile individuare e provare questo tipo di violazioni.

Il software SSH i offre la sicurezza di cui avete bisogno. Il processo di autenticazione, di solito il nome utente e la password e il processo di comunicazione avvengono in forma cifrata; anche qui, è ancora possibile la registrazione dei dati trasmessi ma, a causa della chiave mancante, il contenuto non può venire decodificato. Questo rende possibile una comunicazione sicura attraverso una rete insicuro come internet. SuSE Linux Enterprise Server offre pacchetto `openssh`.

Il pacchetto OpenSSH

Con SuSE Linux per default viene installato il pacchetto OpenSSH. Avrete a vostra disposizione i programmi ssh, scp e sftp, come alternativa per telnet, rlogin, rsh, rcp e ftp.

Il programma ssh

Con ssh, potete stabilire un contatto con un sistema remoto e lavorarci interattivamente. Questo programma sostituisce quindi sia telnet, che rlogin. A causa della sua affinità con rlogin, ssh viene chiamato slogin. Per fare un esempio: con il comando `ssh sole`, si può entrare sul computer `sole` che vi chiederà la vostra password.

Dopo l'autenticazione, potrete lavorare sia dalla riga di comando, che interattivamente, ad esempio, con il programma di amministrazione di SuSE, YaST. Se lo username locale e quello del sistema remoto sono diversi, potete anche indicare un nome differente, ad esempio, `ssh -l agosto sole` o `ssh agosto@sole`.

Inoltre, ssh offre la possibilità, già conosciuta in rsh, di eseguire comandi su un altro sistema. Nel seguente esempio, viene eseguito il comando `uptime` su un computer `sole` e viene creata una directory con il nome `tmp`. L'output del programma avviene sul terminal locale del computer `terra`.

```
tux@terra:~ >  ssh sole "uptime; mkdir tmp"
password di tux@sole:
1:21pm up 2:17, 9 users, load average:  0.15, 0.04, 0.02
```

Le virgolette servono qui per raggruppare due istruzioni in un comando; solo così che verrà eseguito anche il secondo comando sul computer `sole`.

scp – copiare in modo sicuro

Per mezzo di scp potete copiare dei file su un computer remoto. scp è il sostituto cifrato e sicuro per rcp. Per esempio,

```
scp Lamialettera.tex sole:
```

copia il file `lamialettera.tex` dal computer `terra` sul computer `sole`. Se i nomi utente su `terra` e `sole` sono diversi, indicate su scp la formula `nomeutente@nomecomputer`. Non esiste un'opzione `-l`.

Dopo aver immesso la password, scp inizia con la trasmissione dei dati e ne indica lo stato di avanzamento con una barra formata da asterischi e crescente da sinistra a destra. Inoltre, sul margine destro viene mostrato il tempo rimanente (stimato) di trasmissione (ingl. *estimated time of arrival*). Ogni output può venire represso con l'opzione `-q`.

scp offre, oltre alla copia di singoli file, anche un procedimento ricorsivo per la trasmissione di complete directory

```
scp -r src/ sole:backup/
```

copia tutto il contenuto della directory `src/` (comprese le subdirectory) nella sottodirectory `backup/` di `sole`. Se manca, la sottodirectory `backup/` viene creata automaticamente.

Per mezzo dell'opzione `-p`, scp può ricevere la datazione dei file. `-C` provvede ad una trasmissione compressa. In questo modo, viene ridotto al minimo il volume dei dati da trasmettere, anche se questo processo necessita di molta memoria.

sftp - trasmissione più sicura

Alternativamente, si può usare sftp per una più sicura trasmissione dei dati. Entro una sessione, sftp offre molti dei comandi conosciuti in ftp. In confronto ad scp, é vantaggioso soprattutto nella trasmissione di dati i cui nomi di file non sono conosciuti.

Il demone SSH (sshd): la parte del sever

Affinché possano venire utilizzati ssh e scp, i programmi client del pacchetto SSH, deve correre in sottofondo il daemon di SSH, un server. Questi aspetta i suoi collegamenti su TCP/IP port 22.

Durante il primo start, il demone genera tre paia di chiavi. Le paia di chiavi consistono in una parte privata ed una pubblica (ingl. *public*). Per questo, questo procedimento viene definito come procedimento che si basa su una public key. Per garantire la sicurezza della comunicazione con SSH, solo l'amministratore deve poter prendere atto dei file delle chiavi private. A questo scopo, i diritti dei file vengono impostati (preimpostati) in modo molto restrittivo. Le chiavi private sono necessarie solo localmente al daemon SSH e non possono venir date a nessun altro. Le chiavi pubbliche (riconoscibili dall'estensione `.pub`), invece, possono essere date al proprio interlocutore e sono di conseguenza leggibili per tutti gli utenti.

Il client SSH inizia un collegamento. Il demone SSH (in attesa) ed il client SSH (richiedente), si scambiano dati di identificazione, per equiparare la versione di protocollo e software e per escludere il collegamento ad una porta errata. Poiché la risposta viene da un processo figlio (ingl. *child process*) dell'originale demone SSH, sono contemporaneamente possibili diversi collegamenti SSH

Per la comunicazione tra server SSH ed client SSH è a vostra disposizione il protocollo SSH nella versione 1 e 2.

Utilizzando il protocollo SSH versione 1 il server inivia le sue host key pubbliche ed un server key che viene generato ad ogni ora dal demone SSH. Per mezzo delle due chiavi, il client SSH cripta una chiave di sessione, (ingl. *session key*), da lui liberamente scelta e la invia al server SSH: inoltre comunica al server il metodo di crittografia (ingl. *cipher*) usato.

Il protocollo SSH versione 2 fa' a meno della server key. Al suo posto viene utilizzato un algoritmo Diffie-Hellman, per l'interscambio delle chiavi.

Le chiavi private host e server, assolutamente necessarie per la decodificazione della chiave della sessione, non possono venire dedotte dalle parti pubbliche. In questo modo, solo il demone contattato SSH, è in grado di decifrare con la sua chiave privata, la chiave della sessione (cfr. `/usr/share/doc/packages/openssh/RFC.nroff`). Questa fase iniziale di collegamento, può venire facilmente seguita tramite `-v`, l'opzione per la ricerca degli errori, del programma del client SSH. Di default viene utilizzato il protocollo SSH versione 2; con il parametro `-1` potete forzare anche il protocollo SSH versione 1. Se il client archivia tutte le host key pubbliche su `~/.ssh/known_hosts` alla fine della comunicazione, è possibile respingere tutti quegli attacchi del tipo "man-in-the-middle". I server SSH che cercano di

simulare nome ed indirizzo IP di un altro, vengono smascherati per mezzo di un chiaro avviso. Essi si faranno riconoscere dalla chiave host divergente da `~/.ssh/known_hosts` o dal fatto di non riuscire a decifrare la chiave convenuta della sessione, dal momento che gli manca la controparte privata.

E'consigliabile archiviare, all'esterno e ben protette, le chiavi private e pubbliche che si trovano su `/etc/ssh/`. In questo modo, possono venire accertate le modificazioni delle chiavi e, dopo una nuova installazione, possono venire integrate di nuovo le vecchie. Una volta che vi siete assicurati che si tratti del server SSH giusto, eliminate l'impostazione di sistema da `~/.ssh/known_hosts`.

SSH-meccanismi di autenticazione

Ora segue la vera autenticazione, che, nella sua struttura più semplice, consiste nell'inserzione di una password, così come è avvenuta negli esempi sopra citati. Lo scopo di SSH era quello di introdurre un software sicuro e contemporaneamente semplice da usare. Come per i programmi da sostituire rsh e rlogin, anche SSH doveva offrire un metodo semplice di autenticazione. SSH realizza ciò tramite un supplementare paio di chiavi qui creato dall'utente. Allo scopo, il pacchetto SSH offre il programma di aiuto ssh-keygen. Al comando `ssh-keygen -t rsa` o `ssh-keygen -t dsa`, verrà generata la coppia di chiavi e vi verrà richiesto il nome del file di base nel quale memorizzare la chiave:

```
Enter file in which to save the key (/home/tux/.ssh/id_rsa):
```

Confermate il valore di default e fornite anche una passphrase. Anche se il software vi consiglia una passphrase vuota, inserite comunque un testo di 10/30 caratteri. Cercate di non usare parole o frasi semplici o corte. Il programma vi chiederà di inserire la frase una seconda volta. Infine, vi mostrerà dove le chiavi pubbliche e private siano state memorizzate, ovvero, nel nostro esempio, nei file `id_rsa` e `id_rsa.pub`.

```
Enter same passphrase again:
Your identification has been saved in /home/tux/.ssh/id_rsa
Your public key has been saved in /home/tux/.ssh/id_rsa.pub.
The key fingerprint is:
79:c1:79:b2:e1:c8:20:c1:89:0f:99:94:a8:4e:da:e8 tux@sonne
```

Usate `ssh-keygen -p -t rsa` o `ssh-keygen -p -t dsa` per modificare la vostra passphrase. Copiate la parte pubblica della chiave (nel nostro esempio `id_rsa.pub`) sul computer remoto, dove la memorizzerete come

~/.ssh/authorized_keys2. Ogni volta che vi connetterete, vi verrà chiesta la passphrase. In caso contrario, verificate dove siano stati memorizzati i file summenzionati e che il loro contenuto sia corretto.

A lungo andare, questo procedimento è più faticoso dell'inserzione di una password. Di conseguenza, il pacchetto SSH fornisce un altro programma di aiuto, l'ssh-agent, che tiene pronte chiavi private per la durata di una "X session"; a questo scopo, l'X completo, viene avviato come processo figlio dell'ssh-agents. Potete farlo molto semplicemente, impostando su yes la variabile usessh che si trova all'inizio del file .xsession ed eseguite il login tramite un display manager (p.e.KDM o XDM). Alternativamente potete usare ssh-agent startx.

Ora potete utilizzare ssh o scp. Se avete distribuito la vostra chiave pubblica, non dovreste più ricevere la richiesta d'inserimento della password. Quando uscite dal vostro computer, fate attenzione a terminare la vostra X session o di eseguire uno blocco dello schermo protetto da password, per esempio xlock.

Quanto è stato modificato con l'introduzione della seconda versione del protocollo SSH, è riportato nel file /usr/share/doc/packages/openssh/README.SuSE.

Deviazione di X, dell'autenticazione ed altre deviazioni

Oltre ai miglioramenti della sicurezza finora descritti, ssh facilita anche l'uso di applicazioni-X remote. Se inserite ssh con l'opzione -X, sul sistema remoto viene automaticamente impostata la variabile DISPLAY e tutte le emissioni di X vengono deviate, tramite il collegamento ssh, al computer iniziale. Questa comoda funzione impedisce contemporaneamente le possibilità d'intercettazione esistenti finora nelle applicazioni X chiamate su un computer remoto e visualizzate sul computer locale.

Tramite l'opzione impostata -A, il meccanismo di autenticazione ssh-agent viene adottato dal prossimo computer. È così possibile guardare da un computer ad un altro senza dover inserire una password; questo però, solo se prima sono state distribuite e archiviate correttamente le chiavi pubbliche sui computer meta interessati.

Per precauzione, entrambi i meccanismi non sono attivi di default. Per attivarli permanentemente, andate nel file di configurazione del sistema, /etc/ssh/ssh_config o in quello dell'utente ~/.ssh/config.

Potete utilizzare ssh anche per deviare qualsiasi collegamento TCP/IP, ad esempio, la deviazione delle porte SMTP e POP3:

`ssh -L 25:sole:25 sole`. Qui, tramite il canale criptato, ad ogni collegamento a "`terra` Port 25", SMTP viene deviato sulla porta SMTP di `sole`Ciò è utile specialmente per gli utenti di server SMTP che non hanno le facoltà di SMTP-AUTH o POP-before-SMTP. In questo modo, la mail può venire trasmessa da un qualsiasi luogo con collegamento rete e consegnata al mail server "di casa".

In modo analogo `ssh -L 110:sole:110 sole` devia tutte le richieste Port 110, POP3 su `terra` verso la porta POP3 di `sole`.

Entrambi gli esempi devono venire eseguiti come utente `root`, poiché in questo modo si viene collegati su porte locali privilegiate. Con un collegamento SSH già esistente, la posta viene spedita e ritirata (come d'uso) come utente normale. L'host SMTP e POP3 devono venire impostati su `localhost`.

Riceverete ulteriori informazioni dalle pagine di manuale dei singoli programmi e dei file all'indirizzo `/usr/share/doc/packages/openssh`.

Autenticazione della rete — Kerberos

Una rete aperta non offre oltre al comune meccanismo della password – già di per sé non sicurissimo – nessuna altra possibilità che permetta alla workstation di identificare in modo sicuro l'utente. Ciò significa che non è da escludere che un utente appropriandosi dell'identità di un altro possa leggere le e-mail della sua vittima, accedere ai suoi file privati o inizializzare dei processi del sistema. La vostra rete deve soddisfare i seguenti punti per dirsi veramente sicura:

- Gli utenti devono comprovare la propria identità prima di avviare dei servizi del sistema e assicuratevi che nessuno possa assumere l'identità di un altro.
- Inoltre fate in modo che ogni server di rete dia prova della propria identità. Altrimenti un intruso potrebbe riuscire a fingere di essere il server a cui rivolgete le vostre richieste e intercettare informazioni riservate che inviate al server. Per evitare questo vi è la cosiddetta "mutual authentication", ovvero autenticazione reciproca tra client e server.

Kerberos vi aiuta a realizzare quanto descritto sopra tramite l'autenticazione cifrata. I seguenti paragrafi vi mostreranno la procedura da seguire. Comunque verrà descritto solo il modo di funzionamento di Kerberos nei suoi principi. Per maggior dettagli anche di natura tecnica consultate la documentazione acclusa di Kerberos.

Nota

Il Kerberos originario è stato sviluppato al MIT (Massachusetts Institute of Technology). Oltre al MIT Kerberos vi sono anche diverse implementazioni di Kerberos. SuSE Linux Enterprise Server contiene la libera implementazione di Kerberos 5, il cosiddetto Heimdal Kerberos 5 di KTH. Visto che quanto descritto di seguito si riferisce alle caratteristiche comuni delle diverse implementazioni parleremo sempre di Kerberos, fatta eccezione per informazioni specifiche su Heimdal.

Nota

La terminologia di Kerberos

Prima di entrare nei particolari per quanto riguarda Kerberos, diamo uno sguardo al glossario riportato di seguito. Vi aiuterà ad orientarvi nella terminologia di Kerberos.

Credential L'utente o client devono avere dei credenziali che gli conferiscono il diritto di richiedere dei servizi. Kerberos ha due tipi di credenziali — ticket e authenticator.

Ticket Il ticket documenta al server il diritto del client - che cerca di autenticarsi nei confronti dello stesso server - di richiedere dei servizi. Il ticket contiene il nome del server, il nome del client, l'indirizzo Internet del client, e un cosiddetto timestamp, ovvero la datazione del file, la durata di validità e una chiave di sessione (ingl. *session key*) generata casualmente. Questi dati vengono cifrati con la chiave del server.

Authenticator Assieme al ticket viene utilizzato un authenticator per dimostrare che il client che presenta il ticket sia effettivamente quello che dichiara di essere. L'authenticator viene generato in base al nome del client, l'indirizzo IP della workstation e l'orario attuale sulla workstation — cifrato con la chiave di sessione nota solamente al client e al server di cui il client richiede un servizio. Contrariamente al ticket l'authenticator può essere utilizzato una sola volta. Il client può generare un authenticator.

Principal Un Kerberos-Principal è una unità univoca (un utente o un servizio) a cui può essere assegnato un ticket. Un principal è composto da:

- **Primary** – La prima parte del principal che nel caso di un utente può essere identico al nome dell'utente.
- **Instance** – Informazione facoltativa che descrive la primary. Questa catena di caratteri è divisa dalla primary attraverso un '/'.
- **Realm** – Il realm stabilisce la vostra area Kerberos. Di solito il vostro realm è il vostro nome di dominio scritto in maiuscole.

Mutual Authentication Kerberos esegue un processo detto di autenticazione reciproca tra server e client che condividono una chiave di sessione tramite la quale possono comunicare in modo sicuro.

Session Key Le chiavi di sessione sono chiavi private temporanee generate da Kerberos. Sono note al client e vengono utilizzate per cifrare la comunicazione tra client e server, da cui il client ha ottenuto un ticket dopo averlo richiesto.

Replay Quasi tutti i messaggi che vengono inviati in una rete possono essere intercettati, sottratti e inviati nuovamente. Per quanto riguarda Kerberos questo potrebbe rilevarsi pericoloso se l'intruso dovesse riuscire a intercettare le vostre richieste di servizi contenenti il vostro ticket ed authenticator. Potrebbe tentare di inviarle nuovamente ("replay") e spacciarsi per voi. Comunque Kerberos implementa diverse meccanismi per prevenire questa eventualità.

Server o Service "Service" viene utilizzato se deve essere eseguita una determinata azione. Il processo su cui si basa viene chiamato "Server".

Come funziona?

Kerberos viene spesso chiamato anche servizio di autenticazione "Trusted Third Party" che indica che i client, per quanto riguarda l'identità di un altro client, confidano nella valutazione di Kerberos. Kerberos gestisce una banca dati con tutti gli utenti e le loro chiavi private.

Per rilevarsi degno della fiducia Kerberos, il server di autenticazione e il server ticket-granting devono girare su una macchina dedicata. Fate in modo che solo l'amministratore possa accedervi localmente e tramite rete e limitate il più possibile i servizi di rete che girano su questo server — non inizializzate neanche sshd.

Il primo contatto Usare per la prima volta Kerberos assomiglia al login di un comune sistema di rete. Immettete il vostro nome utente. Queste

informazioni e il nome del servizio che mette a disposizione il ticket (ingl. ticket granting services) vengono inviate al server di autenticazione (Kerberos). Se il server di autenticazione vi (ri)conosce, genera una chiave di sessione casuale per l'ulteriore comunicazione tra il vostro client ed il server che mette a disposizione il ticket. A questo punto il server di autenticazione creerà a sua volta un ticket per il server che mette a disposizione i ticket (ticket granting server). Il ticket contiene le seguenti informazioni — tutte cifrate con una chiave di sessione conosciuta solo dal server di autenticazione e quello di ticket granting:

- il nome del client e del ticket granting server
- l'orario
- il durata di validità assegnata al ticket
- l'indirizzo IP del client
- la nuova chiave di sessione appena generata

Successivamente il ticket viene rimandato assieme alla chiave di sessione in forma cifrata al client, però utilizzando la chiave privata del client. Questa chiave privata è nota solo a Kerberos e al client, visto che è stata derivata dalla password dell'utente. Non appena il client ottiene questa risposta, vi verrà chiesta la vostra password. La password verrà convertita in una chiave che può decifrare il pacchetto inviato dal server di autenticazione. Il pacchetto viene "scompattato", e sia la password che la chiave vengono cancellate dalla memoria della workstation. La vostra workstation può comprovare la vostra identità per la durata della validità del ticket che vi permette di ricevere altri ticket (ticket granting) .

Richiesta di un servizio Per poter richiedere un servizio da un server qualsiasi nella rete, l'applicazione del client deve dimostrare la sua identità. Così l'applicazione genera un authenticator che è composto da:

- il principal del client
- l'indirizzo IP del client
- l'ora attuale
- la somma di prova (determinata dal client)

Tutte queste informazioni vengono cifrate con la chiave di sessione che il client ha già ricevuto per questo server in particolare. L'authenticator e il ticket per il server vengono inviati al server. Il server utilizza la propria copia della chiave di sessione per decifrare l'authenticator che

gli fornisce una serie di informazioni necessarie sul client richiedente il servizio. Queste informazioni vengono comparate a quelle contenute nel ticket. Se sul lato server non vi fossero delle misure di sicurezza, questo passaggio sarebbe quello ideale per sferrare un attacco replay. Qualche pirata della rete potrebbe tentare di inviare nuovamente una richiesta che è stata sottratta precedentemente dalla rete. Per evitare ciò il server non accetta richieste con una datazione e ticket già ricevuti in precedenza. Inoltre possono essere rifiutate le richieste la cui datazione si discosta di tanto dal momento nel quale la richiesta è stata ricevuta.

Autenticazione reciproca L'autenticazione di Kerberos può essere impiegata in entrambi le direzioni. Non si tratta solo di stabilire se il client è veramente quello che dichiara di essere; anche il server dovrebbe essere in grado di autenticarsi di fronte al client che richiede la messa a disposizione di un servizio. Così anche lui (il server) invia una specie di authenticator. Aggiunge 1 alla somma di prova ottenuta nell'authenticator del client ed esegue la cifratura con la chiave della sessione condivisa con il client. Il client considera questa risposta come prova della veracità dell'identità del server, e può avere inizio lo scambio di dati tra client e server.

Ticket-Granting — presa di contatto con tutti i server Un server utilizza un ticket; questo significa che appena richiedete un altro servizio avrete bisogno di un nuovo ticket. Kerberos implementa un meccanismo per fornire ticket ai singoli server. Questo servizio viene chiamato "Ticket-Granting Service" che si potrebbe tradurre con: servizio di emissione di ticket. Questo servizio è un servizio come tutti gli altri e sottosta di conseguenza agli stessi protocolli di accesso sovramenzionati. Ogni volta che ad una applicazione serve un ticket, per cui non vi sono altre richieste, essa entra in contatto con il server per l'emissione dei ticket. La richiesta è composta da:

- il principal richiesto
- il ticket per il ticket granting
- l'authenticator

Come nel caso di ogni altro server, il ticket granting server verifica il ticket per il ticket granting e l'authenticator. Se vengono riconosciuti come validi, il server di ticket granting genera una nuova chiave di sessione per l'utilizzo da parte del client originario e il nuovo server. Successivamente viene generato il ticket per il nuovo server contenente le seguenti informazioni:

- il principal del client
- il principal del server
- l'ora attuale
- l'indirizzo IP del client
- la chiave di sessione appena generata

Al nuovo ticket viene assegnato un periodo di validità che corrisponde al rimanente periodo di validità del ticket di ticket granting o al valore standard per il servizio, a seconda di cosa è più breve. Questo ticket e la chiave di sessione vengono inviati al client dal servizio di emissione di ticket. Questa volta però la risposta è stata cifrata dalla chiave di sessione che è stata ricevuta assieme all'originale ticket di ticket granting. Quando viene richiesto un altro servizio, il client è in grado di decifrare la risposta senza richiedere nuovamente la password dell'utente. In questo modo Kerberos ottiene per il client un ticket dopo l'altro senza che l'utente debba eseguire login multipli.

Compatibilità con Windows 2000 Windows 2000 contiene una implementazione Microsoft di Kerberos 5. Visto che SuSE Linux Enterprise Server usa l'implementazione Heimdal di Kerberos 5, nella documentazione di Heimdal troverete sicuramente delle utili informazioni ed istruzioni; vedi *Ulteriori informazioni su Kerberos* nella pagina successiva.

Kerberos e l'utente

Nel caso ideale l'utente viene confrontato con Kerberos solo al momento del login sulla sua workstation. Al login si ottiene un ticket di ticket granting; al logout i ticket Kerberos dell'utente vengono distrutti automaticamente per evitare che altri utenti possano spacciarsi per questo utente quando questi è uscito dal sistema. Il fatto che i ticket vengono distrutti automaticamente comporta delle difficoltà se la sessione dell'utente supera nella durata il periodo di validità assegnato al ticket di ticket granting (10 ore sono un buon valore indicativo). L'utente può ottenere un nuovo ticket di ticket granting, inizializzando kinit. Basta immettere nuovamente la password — Kerberos farà in modo che l'utente potrà accedere ad ogni servizio che richiede senza dover autenticarsi di nuovo. Coloro che sono interessati ad un elenco di tutti i ticket che Kerberos ha ottenuto per voi in sottofondo, utilizzate klist.

Segue una selezione di applicazioni che utilizzano l'autenticazione Kerberos. Queste applicazioni si trovano sotto `/usr/lib/heimdal/bin`. Tutte queste applicazioni offrono tutte le funzionalità delle applicazioni simili

UNIX/Linux ed inoltre il vantaggio di una autenticazione trasparente grazie a Kerberos:

- telnet/telnetd
- rlogin
- rsh, rcp, rshd
- popper/push
- ftp/ftpd
- su
- imapd
- pine

Come noterete non dovrete immettere la vostra password per poter utilizzare queste applicazioni, poiché Kerberos ha già dimostrato la vostra identità. ssh — se compilato per supportare Kerberos — riesce addirittura ad inoltrare ad un'altra postazione di lavoro tutti i ticket che avete ottenuto per una determinata postazione di lavoro. Se utilizzate ssh per fare il login su di un'altra postazione di lavoro, ssh adatterà i contenuti cifrati dei ticket alla nuova situazione. Non basta copiare i ticket semplicemente da una postazione all'altra, visto che il ticket contente informazioni specifiche della postazione (l'indirizzo IP). XDM e KDM supportano anche Kerberos. Leggete nella *Kerberos V5 UNIX User's Guide* all'`http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html` di piü sulle applicazioni di rete di Kerberos.

Ulteriori informazioni su Kerberos

SuSE Linux Enterprise Server contiene la libera implementazione di Kerberos, chiamata Heimdal. La documentazione relativa viene installata con il pacchetto `heimdal` sotto `/usr/share/doc/packages/heimdal/doc/heimdal.info`. La documentazione si trova anche su Internet: `http://www.pdc.kth.se/heimdal/`.

Sulla pagina web ufficiale di della implementazione Kerberosdel MIT trovate dei link su altre risorse relative a Kerberos:
`http://web.mit.edu/kerberos/www/`

Un dialogo cosiddetto classico che spiega il modo di funzionare di Kerberos non vertente esclusivamente sugli aspetti tecnici ma molto interessante si trova sotto:
`http://web.mit.edu/kerberos/www/dialogue.html`

Questo documento spiega il fondamentale funzionamento di Kerberos in modo ben comprensibile. Inoltre contiene una serie di indicazioni per trovare ulteriori fonti di informazione su Kerberos:
`ftp://athena-dist.mit.edu/kerberos/doc/usenix.PS`

Nelle URL riportate di seguito trovate una introduzione a Kerberos

Risposte a tante domande concernenti l'installazione, configurazione e amministrazione di Kerberos:
`http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html`
`http://www.lns.cornell.edu/public/COMP/krb5/install/install_toc.html`
`http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/admin_toc.html`
Le FAQ su Kerberos-FAQ:
`http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html`

Tung, Brian: *Kerberos — A Network Authentication System*. Addison Wesley, 1999. - (ISBN 0-201-37924-4) cd

Installare e amministrare Kerberos

Questa sezione tratta l'installazione della implementazione Kerberos Heimdal e alcuni aspetti riguardanti l'amministrazione. Comunque, si parte dal presupposto che disponete già delle nozioni basilari di Kerberos (vedi anche la sezione *Autenticazione della rete — Kerberos* a pagina 303).

Selezionare i realm di Kerberos

Il "domain" di Kerberos viene chiamato realm e viene identificato con un nome del tipo `FOOBAR.COM` o semplicemente `ACCOUNTING`. Kerberos distingue tra maiuscole e minuscole, dunque foobar.com è un realm diverso da `FOOBAR.COM`. Usate le maiuscole o minuscole secondo le vostre preferenze. Comunque di solito vengono usate le maiuscole per nomi di realm.

Si può usare anche il vostro nome di dominio (o sottodominio p.e. `ACCOUNTING.FOOBAR.COM`). Come vedremo di seguito, se siete un amministratore di sistema potete semplificarvi la vita se configurate i client Kerberos

in modo che accedono al servizio KDC e altri servizi di Kerberos via DNS. Per realizzare ciò è bene che il nome del realm sia un sottodominio del vostro nome di dominio DNS.

Diversamente dallo spazio di nome DNS, Kerberos non è gerarchico. Non potete settare un realm nominato `FOOBAR.COM`, avere due "sottorealm" nominati `DEVELOPMENT` e `ACCOUNTING` e aspettarvi che i due realm subordinati ereditano in qualche modo i principal da `FOOBAR.COM`. Avrete invece tre realm a sé stanti per i quali dovreste configurare l'autenticazione "crossrealm" per utenti di un realm per interagire con server o altri utenti di altri realm.

Per motivi di semplicità partiamo dal presupposto che settate solo un realm per l'intera azienda o simile. Come settare l'autenticazione crossrealm è descritto p.e. in [Tun99]. In questa sezione useremo in tutti gli esempi il nome di realm `SAMPLE.COM`.

Impostare l'hardware KDC

La prima cosa che vi serve per poter usare Kerberos è una macchina che funge da Key Distribution Center abbreviato con KDC che conterrà l'intera banca dati degli utenti di Kerberos assieme alle password e tutte le altre informazioni.

Il KDC è la parte più importante dell'intera infrastruttura di sicurezza — se qualcuno riesce ad entrarvi, tutti gli account degli utenti e tutta l'infrastruttura protetta da Kerberos è compromessa. Un hacker con accesso alla banca dati di Kerberos può assumere le sembianze di un principal qualsiasi nella banca dati! Fate in modo che ciò non possa avvenire:

- Mettete il server in un posto sicuro per esempio in una stanza per server sotto chiave a cui hanno accesso solo pochissime persone.
- Dedicate il server esclusivamente al KDC. Questo vale sia per server che per client — il KDC per esempio non dovrebbe importare alcun filesystem tramite NFS o non dovrebbe usare DHCP per ottenere la propria configurazione di rete.

  Si consiglia di installare prima il sistema minimale, controllare poi la lista dei pacchetti installati e rimuovere i pacchetti non necessari che in particolare sono server come inetd, portmap e cups e tutto quanto si basi su X11. Anche installare un server SSH è da considerarsi un potenziale rischio di sicurezza.

Non è possibile eseguire un login grafico su questa macchina perché un X server rappresenta un fattore di potenziale rischio per la sicurezza. Kerberos ha una propria interfaccia di amministrazione.

- Configurate `/etc/nsswitch.conf` in modo che usi solo file locali per il lookup di utenti e gruppi. Modificate le righe per `passwd` e `group` nel seguente modo:

```
passwd:         files
group:          files
```

  Editate i file `passwd`, `group`, `shadow` e `gshadow` in `/etc` e cancellate le righe che iniziano con un `+` (per richieste NIS).

  Considerate anche la possibilità di disabilitare richieste DNS per motivi di sicurezza. Se nella libreria resolver di DNS vi è un baco di sicurezza, qualcuno potrebbe fare in modo che il KDC esegui una richiesta DNS che sfrutta questo baco. Per disabilitare lookup DNS rimuovete semplicemente `/etc/resolv.conf`.

- Disabilitate tutti gli account degli utenti fatta eccezione per l'account di root editando `/etc/shadow` e sostituendo con `*` o `!` le cosiddette hash delle password.

Sincronizzazione dell'orologio

Per usare Kerberos in modo efficace provvedete a sincronizzare l'orario dei sistemi. La ragione è che Kerberos cerca di proteggervi da cosiddetti credenziali "replayed" ovvero inviati più volte. Un intruso potrebbe intercettare i credenziali di Kerberos nella rete e riutilizzarli per sferrare degli attacchi contro il server. Kerberos implementa diversi meccanismi per prevenire questa eventualità. Uno dei quali consiste nel aggiungere dei time stamp ovvero la datazione ai propri ticket. Un server che riceve un ticket con una datazione che si discosta da quella attuale rifiuterà il ticket.

Chiaramente Kerberos consente una certa discrepanza tra le datazioni. Comunque gli orologi dei computer possono essere poco precisi nel scandire il tempo — non accade di rado che orologi di PC guadagno o perdono mezz'ora nell'arco di una settimana rispetto all'orario di riferimento. Si consiglia dunque di configurare tutti gli host nella rete in modo che si sincronizzano all'orario centrale.

Un modo semplice è quello di installare un time server NTP su una macchina e sincronizzare l'orario dei vari client a quello di questo server,facendo girare un demone NTP nel modo client su tutte le macchine o fare eseguire `ntpdate` una volta al giorno da tutti i client (questa soluzione probabilmente funzionerà solo se avete un numero ristretto di client).

Anche il KDC deve essere sincronizzato sull'orario centrale. Far girare un demone NTP su questa macchina rappresenterebbe un rischio per la sicurezza, per questo si consiglia di sincronizzare l'ora lanciando ntpdate attraverso una registrazione cron.

La configurazione dell'NTP non rientra nel quadro di questa sezione, per avere ulteriori informazioni consultate la documentazione su NTP acclusa sotto `/usr/share/doc/packages/xntp-doc`

Configurazione di log

Di default, i demoni Kerberos che girano sull'host KDC protocolleranno l'informazione nel demone syslog. Se volete tenere sott'occhio l'attività di KDC, controllate questi file di protocollo ad intervalli regolari per vedere si verificano strani eventi o se vi sono dei potenziali problemi, eseguendo uno script di scansione di log sullo stesso host KDC o copiando questi file dal KDC su un altro host via rsync ed analizzando lì i log. Si sconsiglia di inoltrare l'output di log tramite il meccanismo di inoltro di syslogd, perché le informazioni attraversano la rete in forma non cifrata.

Installare il KDC

In questa sezione verrà descritta l' installazione di KDC e la generazione di un principal amministrativo.

Installare gli RPM

Innanzitutto bisogna installare il software Kerberos. Installate gli rpm `heimdal` e `heimdal-lib` sul KDC:

```
terra:~ #  rpm -ivh heimdal-0*.rpm heimdal-lib-0*.rpm
```

Editare krb5.conf

Poi editate il file di configurazione `/etc/krb5.conf`. Il file viene installato di default e contiene diverse registrazioni campione. Assicuratevi di aver cancellate tutte queste registrazioni prima di incominciare.

`krb5.conf` è composto da diversi sezioni, ognuna introdotta dal nome di sezione in parentesi `[così]`. L'unica sezione importante per il momento è `[libdefaults]`, che dovrebbe essere simile a quanto riportato di seguito:

```
[libdefaults]
      default_realm = SAMPLE.COM
          clockskew = 300
```

La riga `default_realm` setta il realm di default per le applicazioni Kerberos. `clock_skew` definisce il periodo di tolleranza di accettazione dei ticket con datazione che non corrisponde esattamente l'ora dell'host KDC. Di solito tale valore è di 300 secondi che equivalgono a 5 minuti. Questo significa che il ticket può avere una datazione che si discosta di 5 minuti sia prima che dopo dall'orario del server. Se usate NTO per sincronizzare tutti gli host potete ridurre questo valore di ca. un minuto.

Impostare la cosiddetta chiave master

Ora dovete inizializzare la banca dati nella quale Kerberos raccoglie tutte le informazioni sui principal. Innanzitutto impostate la chiave master utilizzata per proteggere la fuga accidentale di informazioni dal banca di dati, in particolare quando si esegue un back-up su nastro.

La chiave master viene derivata dalla pass phrase e viene memorizzata in un file chiamato stash file. Non è necessario che immettete la password ad ogni riavvio di KDC. Scegliete la pass phrase con accortezza, p.e. la frase di un libro che si trova su una pagina che avete aperto a caso.

Quando fate delle copie di sicurezza su nastro della banca dati di Kerberos (`/var/heimdal/heimdal.db`), non fatene dello stash file (che è in `/var/heimdal/m-key`). Altrimenti chiunque è in grado di leggere il nastro potrebbe anche decifrare la banca dati. Per questo motivo è consigliabile di tenere una copia della pass phrase in un luogo sicuro, visto che vi servirà quando dovrete ripristinare dal nastro la banca dati dopo un crash.

Per impostare la chiave master, invocate l'utility kstash senza argomenti ed immettete la pass phrase due volte:

```
terra:~ #  kstash

Master key:<enter pass phrase>
Verifying password - Master key:<enter pass phrase again>
```

Generare il realm

In fine immettete le vostre registrazioni per il realm nella banca dati di Kerberos. Richiamate l'utility kadmin con l'opzione -l come mostrato sopra. Questa opzione istruisce kadmin di accedere la banca dati localmente. Di default cercherà di contattare il servizio admin di Kerberos tramite la rete che al momento non funzionarà, visto che non è stata impostata.

Ora date a kadmin l'istruzione di inizializzare il vostro realm. Vi verranno poste una serie di domande. All'inizio si consiglia di accettare quanto impostato di default da kadmin:

```
terra:~ #  kadmin -l


kadmin> init SAMPLE.COM
Realm max ticket life [unlimited]: <press return>
Realm max renewable ticket life [unlimited]: <press return>
```

Per verifica cosa è accaduto, usate il comando list:

```
kadmin> list *
default@SAMPLE.COM
kadmin/admin@SAMPLE.COM
kadmin/hprop@SAMPLE.COM
kadmin/changepw@SAMPLE.COM
krbtgt/SAMPLE.COM@SAMPLE.COM
changepw/kerberos@SAMPLE.COM
```

Vi indica che vi sono una serie di principal nella banca dati per l'uso proprio di Kerberos.

Generare un principal

Ora generate due principal Kerberos per voi stessi: un principal "normale" per le mansioni quotidiane e uno per compiti amministrativi riguardanti Kerberos. Assumendo che il vostro nome di login sia `newbie`, procedete come di seguito:

```
terra:~ #  kadmin -l


kadmin> add newbie
Max ticket life [1 day]: <press return>
Max renewable life [1 week]: <press return>
Principal expiration time [never]: <press return>
```

```
Password expiration time [never]: <press return>
Attributes []: <press return>
newbie@SAMPLE.COM's Password: <type password here>
Verifying password: <re-type password here>
```

Va bene accettare i valori di default premendo (Enter). Scegliete una buona password.

Dopo generate un altro principal chiamato `newbie/admin` inserendo `add newbie/admin` al prompt di `kadmin`. L'`admin` aggiunto al vostro nome utente viene chiamato role che userete per amministrare la banca dati di Kerberos.

Impostare l'amministrazione da remoto

Per poter aggiungere e rimuovere principal dalla banca dati di Kerberos senza usare direttamente la console di KDC, comunicate al server admin di Kerberos quali principal sono provvisti del permesso di farlo.

Editate a riguardo il file `/var/heimdal/kadmind.acl` (ACL sta per Access Control List). Il file ACL vi permette di stabilire i permessi in modo mirato. Per i dettagli, vedi pagina di manuale di `kadmind` (`man 8 kadmind`).

Conferitevi il permesso di fare tutto ciò volete con la banca dati inserendo la seguente riga nel file:

```
newbie/admin              all
```

Sostituite il nome utente `newbie` con il vostro.

Avviare il KDC

Avviate i demoni KDC. Anche lo stesso kdc (che gestisce le richieste di autenticazione degli utenti e dei ticket), kadmind (il server per l'amministrazione da remoto) e kpasswddd (che gestisce le richieste di modifica della password dell'utente). Per avviare il demone manualmente, inserite:

```
terra:~ #  rckdc start

Starting kdc              done
```

Assicuratevi che il KDC venga avviato di default quando il server viene riavviato. Il comando è `insserv kdc`.

Configurare client Kerberos

Ci sono due vie da seguire quando configurate Kerberos — configurazione statica tramite il file `/etc/krb5.conf` o configurazione dinamica tramite DNS. Nella variante DNS, le applicazioni di Kerberos cercheranno di accedere ai servizi di KDC tramite registrazioni DNS. Mentre nell'approccio statico dovete aggiungere i nomi degli host del vostro server KDC su `krb5.conf` (e aggiornare il file ogni volta che spostate il KDC o riconfigurate il vostro realm).

La configurazione DNS è in genere molto più flessibile e il carico amministrativo per macchina è considerevolmente inferiore. Comunque il nome di realm deve essere lo stesso del vostro dominio DNS o di un sottodominio di esso.

Configurare Kerberos tramite DNS inoltre crea un piccolo rischio di sicurezza: un intruso potrebbe danneggiare seriamente la vostra infrastruttura attraverso DNS (shoot down il server dei nome server, spoofing di registrazioni DNS, etc). Comunque ciò corrisponde ad un denial of service. Qualcosa di simile può accadere nel caso della configurazione statica, a meno che non immettiate indirizzi IP non cifrati in krb5.conf al posto di nomi degli host.

La configurazione statica

Nel caso della configurazione statica, aggiungete le seguenti righe a `krb5.conf` (`kdc.sample.com` è il nome dell' host di KDC):

```
[realms]
   SAMPLE.COM = {
            kdc = kdc.sample.com
 kpasswd_server = kdc.sample.com
   admin_server = kdc.sample.com
        }
```

Se avete diversi realm, aggiungete semplicemente un ulteriore statement alla sezione `[realms]`.

Aggiungete anche una istruzione che indichi alle applicazioni come mappare nomi degli host nel realm. Per esempio quando vi connettete a un host remoto, la libreria Kerberos deve sapere in quale realm si trovi l'host. Ciò va impostato nella sezione `[domain_realms]`:

```
[domain_realm]
        .sample.com = SAMPLE.COM
     www.foobar.com = SAMPLE.COM
```

Questo indica alla libreria che tutti gli host nei domini DNS `sample.com` si trovano nel realm di Kerberos `SAMPLE.COM`. Inoltre un host esterno di nome `www.foobar.com` dovrebbe anch'esso essere considerato un membro del realm `SAMPLE.COM`.

La configurazione DNS

Nella configurazione basata su DNS di Kerberos vengono usate tante registrazioni SRV (vedi *(RFC2052) A DNS RR for specifying the location of services* sotto `http://www.ietf.org`). Queste registrazioni non vengono supportate da implementazioni precedenti del server dei nomi BIND. Lo sono a partire dalla versione 8 di BIND.

La registrazione SRV, per quanto riguarda Kerberos, è del tipo: `_service._proto.realm`, laddove realm è il realm di Kerberos. Tenete presente che nei nomi di dominio di DNS non si distingue tra maiuscole e minuscole, così i realm di Kerberos crashano in concomittanza con questo metodo di configurazione. `_service` è un nome di servizio (vengono usati differenti nomi quando si cerca per esempio di contattare il KDC o il servizio password). `_proto` può assumere il valore `_udp` o `_tcp`, ma non tutti i servizi supportano entrambi i protocolli.

La parte dei dati delle registrazioni di risorse SRV consistono di un valore di priorità, ponderazione, un numero di porta ed di un nome di host. La priorità definisce l'ordine nel quale gli host devono essere contatti (valori bassi indicano un'alta priorità). Il peso supporta il load balancing tra server di egual priorità. Probabilmente non vi servirà alcuno, così potete impostare qui zero.

Heimdal Kerberos cerca i seguenti nomi quando cerca di rilevare dei servizi:

`_kerberos` definisce la locazione del demone KDC (il server di autenticazione e di ticket granting). Delle registrazioni tipiche hanno il seguente aspetto:

```
_kerberos._udp.SAMPLE.COM.  IN  SRV    0 0 88 kdc.sample.com.
_kerberos._tcp.SAMPLE.COM.  IN  SRV    0 0 88 kdc.sample.com.
```

`_kpasswd` descrive la locazione del server che modifica la password. Registrazioni tipiche sono simili a quanto segue:

```
_kpasswd._udp.SAMPLE.COM.   IN  SRV    0 0 464 kdc.sample.com.
```

Visto che kpasswdd non supporta TCP, non ci dovrebbe essere registrazioni `_tcp`.

`_kerberos-adm` descrive la locazione del servizio di amministrazione remoto. Ecco delle registrazioni tipiche:

```
_kerberos-adm._tcp.SAMPLE.COM. IN  SRV    0 0 749 kdc.sample.com.
```

Visto che kadmind non supporta UDP, non ci dovrebbero essere registrazioni `_udp`.

Come per il caso del file di configurazione statico, vi è un meccanismo che informa i client che un host specifico si trova nel realm `SAMPLE.COM`, anche se fa parte del dominio DNS sample.com. Questo può essere realizzato aggiungendo una registrazione TXT a `_keberos.hostname`, come mostrato di seguito:

```
_keberos.www.foobar.com.  IN TXT "SAMPLE.COM"
```

Gestire i principal

Il tool kadmin vi permette di amministrare Kerberos da remoto. Innanzitutto si rende necessario un ticket per il vostro admin principal da usare quando vi collegate al server kadmin:

```
terra:newbie #  kinit newbie/admin

newbie/admin@SAMPLE.COM's Password: <enter password>

terra:newbie #  /usr/sbin/kadmin

kadmin> privs
change-password, list, delete, modify, add, get
```

Con il comando privs potete verificare i permessi di cui disponete. La lista indicata sopra riporta tutti i permessi.

Modificate per esempio il principal `newbie`:

```
kadmin> mod newbie
Max ticket life [1 day]:2 days
Max renewable life [1 week]:
Principal expiration time [never]:2003-01-01
Password expiration time [never]:
Attributes []:
```

Questo modifica la validità massima del ticket life a due giorni e imposta la data di scadenza per l'account sul primo gennaio del 2003.

I comandi principali di kadmin sono:

add ⟨***principal***⟩ aggiunge un nuovo principal

modify ⟨***principal***⟩ edita diversi attributi di un principal, come la validità massima del ticket e la scadenza dell'account

delete ⟨***principal***⟩ rimuove un principal dalla banca dati

rename ⟨***principal***⟩ ⟨***nuovo nome***⟩ cambia il nome del principal in ⟨*nuovo nome*⟩

list ⟨***pattern***⟩ elenca tutti i principal che corrispondono a determinate caratteristiche. I pattern funzionano alla stregua dei pattern globbing della shell: `list newbie*` elencherebbe `newbie` e `newbie/admin` nel nostro esempio.

get ⟨***principal***⟩ mostra informazioni dettagliata sul principal

passwd ⟨***principal***⟩ cambia la password del principal

Potete ricevere assistenza in ogni momento premendo su ? e Enter, o dai prompt emessi da comandi come modifica o aggiungi.

Il comando `init` (e pochi altri) non è disponibile nella modalità remota se usato quando viene generato il realm. Per generare un nuovo realm, andate sulla console di KDC e usate kadmin nella modalità locale (con l'opzione di riga di comando `-l`).

Abilitare il supporto PAM per Kerberos

SuSE Linux Enterprise Server contiene il modulo PAM `pam_krb5` che supporta il login e l'aggiornamento della password Kerberos. Questo modulo può essere utilizzato da applicazioni, come la console di login, su e applicazioni per il login grafico come KDM, dove l'utente immette una password e si aspetta di ottenere una chiave Kerberos iniziale dalla applicazione di autenticazione. Per consentire agli utenti di aggiornare in modo trasparente la loro password Kerberos servendosi dell'utility standard passwd (invece di ricorrere al programma kpasswd), aggiungete inoltre `pam_krb5` alla configurazione PAM di passwd.

Il modulo `pam_krb5` **non** è stato concepito per servizi di rete che accettano ticket di Kerberos quale parte della autenticazione dell'utente.

In ogni caso, editate i file di configurazione PAM di questi servizi a cui aggiungere il supporto di Kerberos. Le seguenti applicazioni possono usare `pam_krb5`. Sono elencati anche i rispettivi file di configurazione PAM.

```
login                   /etc/pam.d/login
su                      /etc/pam.d/su
kdm, gdm, xdm           /etc/pam.d/xdm
xlock                   /etc/pam.d/xlock
passwd                  /etc/pam.d/passwd
```

Usare pam_krb5

Potete usare `pam_krb5` in due modi, dipende se volete fare di KDC il metodo di autenticazione primario e usate le password della banca dati delle password tradizionale solo come fallback o se volete usare la banca dati tradizionale quale sorgente primaria e usare `pam_krb5` solo per ricevere ticket Kerberos per gli utenti coi principal nel KDC. Il secondo approccio è particolarmente indicato per la fase di migrazione da un altro meccanismo di autenticazione verso Kerberos.

Dato che Kerberos si occuperà esclusivamente dell'autenticazione, avrete inoltre bisogno di un meccanismo per distribuire le rimanenti informazioni di account come l'uid e la directory home. Uno di questi meccanismi è LDAP. Utilizzare NIS non è un'alternativa, poiché Linux attualmente non supporta alcun meccanismo di sicurezza Kerberos per servizi di rete RPC.

Optional pam_krb5

In questa modalità l'autenticazione primaria avvinen tramite il framework di autenticazione esistente, come le registrazioni degli utenti nel file `/etc/passwd` o nella banca dati NIS. L'unica differenza è che all'utente viene associato inoltre un principal di Kerberos e che `pam_krb5` tenterà di ottenere un ticket per l'utente, usando la password fornita in precedenza.

Considerate per esempio il file di configurazione PAM per su, che contiene queste righe per il servizio `auth` :

```
auth     sufficient     pam_rootok.so
auth     required       pam_unix.so     nullok
```

Queste due righe comunicano alla libreria di PAM che all'autenticazione dell'utente dovrebbe richiamare innanzitutto il modulo `pam_rootok`. Se riesce (ovvero se l'utente richiedente è l'utente root), la richiesta di su dovrebbe essere accettata senza ulteriori richieste di autenticazione. Altrimenti

PAM continua e richiama il modulo pam_unix che esegue l'autenticazione "tradizionale" richiedendo dall'utente la password, eseguendo un hash della password e compararla alla password già sottoposta all'hash dell'account dell'utente di destinazione.

Per aggiungere il supporto facoltativo di Kerberos, aggiungete un'altra riga dopo di questa nel seguente modo:

```
auth     optional       pam_krb5.so     try_first_pass \
                                        missing_keytab_ok \
                                        ccache=SAFE \
                                        putenv_direct
```

che richiama il modulo pam_krb5 e ignora gli errori marcati (per esempio, quando non è riuscito ad aver un ticket per l'utente). In questa impostazione la password viene sempre comparata alle registrazioni di password nel framework di autenticazione originale.

Per gli altri servizi, le modifiche apportate al file di configurazione PAM sono simili. La cosa migliore è aggiungere la riga pam_krb5 dopo quella che chiama pam_unix o pam_unix2.

Usare pam_krb5 per l'autenticazione primaria

Se avete portato tutti gli utenti su Kerberos, potete usare pam_krb5 come meccanismo di autenticazione primario e ripiego per il file password locale se si verifica un errore, per esempio non vi è un principal per questo utente o il KDC è momentaneamente fuori uso. Con questa impostazione tutti gli account degli utenti sarebbero di default nella banca dati di Kerberos e il ripiego per il file delle password locale esiste solo per gli account come quello di root.

Il seguente esempio indica come modificare /etc/pam.d/su per realizzare ciò (notate l'argomento aggiuntivo use_first_pass per il modulo pam_unix):

```
auth     sufficient     pam_rootok.so
auth     sufficient     pam_krb5.so     missing_keytab_ok \
                                                ccache=SAFE \
                                                putenv_direct
auth     required       pam_unix.so     use_first_pass nullok
```

Questa modifica inserisce pam_krb5 prima del modulo pam_unix e lo dichiara come sufficiente il che significa che PAM richiama con successo

pam_krb5 e non ripiegherà a richiamare pam_unix, altrimenti continuerà a richiamare e ripiegare su pam_unix.so.

Comunque non tutte le applicazioni possono essere modificate così facilmente come su. Segue il file PAM per il login (almeno le poche righe riguardanti l'autenticazione):

```
auth    requisite       pam_unix2.so    nullok
auth    required        pam_securetty.so
auth    required        pam_nologin.so
auth    required        pam_env.so
auth    required        pam_mail.so
```

Inserite una riga per pam_krb5 prima di pam_unix2 se l'autenticazione pam_krb5 riesce, saltate pam_unix2 ma continuate con gli altri moduli. E' un pò più complicato di quanto mostrato qui:

```
auth    [success=1 default=ignore] \
                        pam_krb5.so     missing_keytab_ok \
                                        ccache=SAFE \
                                        putenv_direct
auth    requisite       pam_unix2.so    nullok
        ... il resto come sopra ...
```

Così PAM salterà un modulo (pam_unix2) se pam_krb5 comunica la riuscita. Ogni altra risposta viene ignorata e pam_unix2 viene lanciato come prima.

Aggiornare la password con pam_krb5

Se usate Kerberos vi sono di solito due modi per l'utente di aggiornare la propria password — attraverso l'utility kpasswd (che vale solo per password Kerberos) o facendo aggiungere all'amministratore di sistema il modulo pam_krb5 alla configurazione di passwd.

Per realizzare ciò, modificate /etc/pam.d/passwd nel modo seguente:

```
auth     required       pam_krb5.so
account  required       pam_unix2.so
password required       pam_pwcheck.so  nullok
password required       pam_krb5.so
password required       pam_unix2.so    nullok use_first_pass use_authtok
session  required       pam_unix2.so
```

Se usate un servizio directory come LDAP, ma avete tolto le password degli utenti dal LDAP (non è una buona idea avere queste password in LDAP quando usate Kerberos), modificate la configurazione di `passwd` del PAM `passwd` nel seguente modo:

```
auth     required       pam_krb5.so
account  required       pam_unix2.so
password required       pam_pwcheck.so  nullok
password required       pam_krb5.so     nopasswdverify
session  required       pam_unix2.so
```

Configurare un server di rete per Kerberos

Finora abbiamo trattato solo i credenziali degli utenti. Comunque, anche server di rete "Kerberosizzati" di solito devono autenticarsi di fronte all' utente del client. Ovviamente non possono essere usati ticket di Kerberos come per i normali utenti, perché non sarebbe auspicabile per l'amministratore di sistema doversi procurare nuovi ticket per ogni servizio ogni otto ore o qualcosa del genere.

I server di rete invece mantengono le loro chiavi Kerberos in cosiddette keytabs e ottengono nuovi ticket automaticamente quando ne hanno bisogno.

Normalmente avrete bisogno almeno di un principal per ogni host sul quale è in esecuzione un servizio di rete che utilizza Kerberos. Questo principal viene chiamato `host/machine.sample.com@SAMPLE.COM`, dove `machine.sample.com` è il nome di host usuale della macchina server.

Innanzitutto generate il principal. Assicuratevi di avere credenziali admin validi e poi aggiungete il nuovo principal:

```
terra:~ #  kinit newbie/admin

newbie/admin@SAMPLE.COM's Password: <type password>

terra:~ #  kadmin add -r host/machine.sample.com

Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
```

Invece di settare una password per il nuovo principal, il flag -r dice al kadmin di generare una chiave casuale. Possiamo fare ciò per evitare dell'interazioni da parte degli utenti per questo principal. Si tratta di un account di server per la macchina.

Infine estraete la chiave e memorizzatela nel file keytab locale `/etc/krb5.keytab`. Questo file appartiene al superutente, per questo dovete essere root per poter eseguire il prossimo comando:

```
terra:~ #  ktutil get host/machine.sample.com
```

Alla fine assicuratevi di aver distrutto l'admin ticket che avete ottenuto tramite kinit con `kdestroy`.

Configurare sshd per l'autenticazione Kerberos

Per usare sshd con l'autenticazione Kerberos, editate `/etc/ssh/sshd_config` ed impostate le seguenti due opzioni:

```
KerberosAuthentication yes
KerberosTgtPassing yes
```

Riavviate quindi il vostro demone SSH con `rcsshd restart`.

Dovreste essere in grado di connettervi usando l'autenticazione di Kerberos. Kerberos attualmente vien supportato solo se usate il protocollo SSH versione 1; così il client deve selezionare questo protocollo e aggiungere l'opzione `-1` sulla riga di comando

```
terra:newbie #  ssh -1 earth.sample.com


Last login: Fri Aug  9 14:12:50 2002 from zamboni.sample.com
Have a lot of fun...


terra:newbie #
```

Usare LDAP e Kerberos

Per consentire che Kerberos si connetti al server OpenLDAP, generate un principal `ldap/earth.sample.com` e aggiungetelo alla keytab:

```
terra:~ #  kadmin add -r ldap/earth.sample.com
```

```
terra:~ #  ktutil get ldap/earth.sample.com
```

Dopo aver riavviato il server LDAP con `rcldap restart`, dovreste essere in grado di usare automaticamente i tool come ldapsearch per esempio, con l'autenticazione di Kerberos.

```
terra:~ #  ldapsearch -b ou=People,dc=suse,dc=de '(uid=newbie)'
```

```
SASL/GSSAPI authentication started
SASL SSF: 56
SASL installing layers
[...]

# newbie, People, suse.de
dn: uid=newbie,ou=People,dc=suse,dc=de
uid: newbie
cn: Olaf Kirch
[...]
```

Assicuratevi che ldapsearch usi Kerberos per visualizzare messaggi SASL/GSSAPI. GSSAPI è il General Security Services API ed è un interfaccia di programmazione che nasconde alle applicazioni i dettagli di vari meccanismi di autenticazione. SASL è un protocollo di rete che invia informazioni di autenticazione dal client al server e viceversa.

Manual-Page di e2fsck

NAME

e2fsck - check a Linux second extended file system

SYNOPSIS

e2fsck [-pacnyrdfvstFSV] [-b superblock] [-B blocksize] [-l|-L bad_blocks_file] [-C fd] [-j external-journal] [device

DESCRIPTION

e2fsck is used to check a Linux second extended file system (e2fs). E2fsck also supports ext2 filesystems containing a journal, which are also sometimes known as ext3 filesystems.

device is the special file corresponding to the device (e.g /dev/hdc1).

OPTIONS

-a This option does the same thing as the -p option. It is provided for backwards compatibility only; it is suggested that people use -p option whenever possible.

-b superblock

Instead of using the normal superblock, use an alternative superblock specified by superblock. This option is normally used when the primary superblock has been corrupted. The location of the backup superblock is dependent on the filesystem's blocksize. For filesystems with 1k blocksizes, a backup superblock can be found at block 8193; for filesystems with 2k blocksizes, at block 16384; and for 4k blocksizes, at block 32768.

Additional backup superblocks can be determined by using the mke2fs program using the -n option to print out where the superblocks were created. The -b option to mke2fs, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the filesystem is not opened read-only, e2fsck will make sure that the primary superblock is updated appropriately upon completion of the filesystem check.

-B blocksize
Normally, e2fsck will search for the superblock at various different block sizes in an attempt to find the appropriate block size. This search can be fooled in some cases. This option forces e2fsck to only try locating the superblock at a particular blocksize. If the superblock is not found, e2fsck will terminate with a fatal error.

-c This option causes e2fsck to run the badblocks(8) program to find any blocks which are bad on the filesystem, and then marks them as bad by adding them to the bad block inode.

-C This option causes e2fsck to write completion information to the specified file descriptor so that the progress of the filesystem check can be monitored. This option is typically used by programs which are running e2fsck. If the file descriptor specified is 0, e2fsck will print a completion bar as it goes about its business. This requires that e2fsck is running on a video console or terminal.

-d Print debugging output (useless unless you are debugging e2fsck).

-f Force checking even if the file system seems clean.

-F Flush the filesystem device's buffer caches before beginning. Only really useful for doing e2fsck time trials.

-j external-journal
Set the pathname where the external-journal for this filesystem can be found.

-l filename
Add the blocks listed in the file specified by filename to the list of bad blocks. The format of this file is the same as the one generated by the badblocks(8) program.

-L filename
Set the bad blocks list to be the list of blocks specified by filename. (This option is the same as the -l option, except the bad blocks list is cleared before the blocks listed in the file are added to the bad blocks list.)

-n Open the filesystem read-only, and assume an answer of 'no' to all questions. Allows e2fsck to be used non-interactively. (Note: if the -c, -l, or -L options are specified in addition to the -n option, then the filesystem will be opened read-write, to permit the bad-blocks list to be updated. However, no other changes will be made to the filesystem.)

-p Automatically repair ("preen") the file system without any questions.

-r This option does nothing at all; it is provided only for backwards compatibility.

-s This option will byte-swap the filesystem so that it is using the normalized, standard byte-order (which is i386 or little endian). If the filesystem is already in the standard byte-order, e2fsck will take no action.

-S This option will byte-swap the filesystem, regardless of its current byte-order.

-t Print timing statistics for e2fsck. If this option is used twice, additional timing statistics are printed on a pass by pass basis.

-v Verbose mode.

-V Print version information and exit.

-y Assume an answer of 'yes' to all questions; allows e2fsck to be used non-interactively.

EXIT CODE

The exit code returned by e2fsck is the sum of the following conditions:

0 - No errors
1 - File system errors corrected
2 - File system errors corrected, system should be rebooted if file system was mounted
4 - File system errors left uncorrected
8 - Operational error
16 - Usage or syntax error
128 - Shared library error

SIGNALS

The following signals have the following effect when sent to e2fsck.

SIGUSR1

This signal causes e2fsck to start displaying a completion bar. (See discussion of the -C option.)

SIGUSR2

This signal causes e2fsck to stop displaying a completion bar.

REPORTING BUGS

Almost any piece of software will have bugs. If you manage to find a filesystem which causes e2fsck to crash, or which e2fsck is unable to repair, please report it to the author.

Please include as much information as possible in your bug report. Ideally, include a complete transcript of the e2fsck run, so I can see exactly what error messages are displayed. If you have a writeable filesystem where the transcript can be stored, the script(1) program is a handy way to save the output of e2fsck to a file.

It is also useful to send the output of dumpe2fs(8). If a specific inode or inodes seems to be giving e2fsck trouble, try running the debugfs(8) command and send the output of the stat(1u) command run on the relevant inode(s). If the inode is a directory, the debugfs dump command will allow you to extract the contents of the directory inode, which can sent to me after being first run through uuencode(1).

Always include the full version string which e2fsck displays when it is run, so I know which version you are running.

```
AUTHOR
       This  version  of  e2fsck  was  written  by  Theodore Ts'o
       <tytso@mit.edu>.

SEE ALSO
       mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)


E2fsprogs version 1.25    September 2001               E2FSCK(8)
```

La Licenza Pubblica GNU (GPL)

Questa e' una traduzione italiana non ufficiale della Licenza Pubblica Generale GNU. Non e' pubblicata dalla Free Software Foundation e non ha valore legale nell'esprimere i termini di distribuzione del software che usa la licenza GPL. Solo la versione originale in inglese della licenza ha valore legale. Ad ogni modo, speriamo che questa traduzione aiuti le persone di lingua italiano a capire meglio il significato della licenza GPL.

This is an unofficial translation of the GNU General Public License into Italian. It was not published by the Free Software Foundation, and does not legally state the distribution terms for software that uses the GNU GPL–only the original English text of the GNU GPL does that. However, we hope that this translation will help Italian speakers understand the GNU GPL better.

LICENZA PUBBLICA GENERICA (GPL) DEL PROGETTO GNU
Versione 2, Giugno 1991

Copyright (C) 1989, 1991 Free Software Foundation,
Inc. 675 Mass Ave, Cambridge, MA 02139, USA

Traduzione curata dal gruppo Pluto e da
ILS, ultimo aggiornamento, 30 luglio 1998.

Tutti possono copiare e distribuire copie letterali di questo documento di licenza, ma non e' lecito modificarlo.

Preambolo

Le licenze per la maggioranza dei programmi hanno lo scopo di togliere all'utente la liberta' di condividerlo e di modificarlo. Al contrario, la Licenza Pubblica Generica GNU e' intesa a garantire la liberta' di condividere e modificare il free software, al fine di assicurare che i programmi siano "liberi" per

tutti i loro utenti. Questa Licenza si applica alla maggioranza dei programmi della Free Software Foundation e ad ogni altro programma i cui autori hanno scelto questa Licenza. Alcuni altri programmi della Free Software Foundation sono invece coperti dalla Licenza Pubblica Generica per Librerie. Chiunque puo' usare questa Licenza per i propri programmi.

Quando si parla di "free software", ci si sriferisce alla liberta', non al prezzo. Le nostre Licenze (la GPL e la LGPL) sono progettate per assicurarsi che ciascuno abbia la liberta' di distribuire copie del free software (e farsi pagare per questo, se vuole), che ciascuno riceva il codice sorgente o che lo possa ottenere se lo desidera, che ciascuno possa modificare il programma o usarne delle parti in nuovi programmi "liberi" e che ciascuno sappia di potere fare queste cose.

Per proteggere i diritti dell'utente, abbiamo bisogno di creare delle restrizioni che vietino a chiunque di negare questi diritti o di chiedere di rinunciarvi. Queste restrizioni si traducono in certe responsabilita' per chi distribuisce copie del software e per chi lo modifica.

Per esempio, chi distribuisce copie di un Programma coperto da GPL, sia gratis sia in cambio di un compenso, deve dare ai destinatari tutti i diritti che ha ricevuto. Deve anche assicurarsi che i destinatari ricevano o possano ricevere il codice sorgente. E deve mostrar loro queste condizioni di Licenza, in modo che conoscano i loro diritti.

Proteggiamo i diritti dell'utente in due modi: (1) proteggendo il software con un copyright, e (2) offrendo una Licenza che offre il permesso legale di copiare, distribuire e/o modificare il Programma.

Infine, per proteggere ogni autore e noi stessi, vogliamo assicurarci che ognuno capisca che non ci sono garanzie per i programmi coperti da GPL. Se il Programma viene modificato da qualcun altro e ridistribuito, vogliamo che gli acquirenti sappiano che cio' che hanno non e' l'originale, in modo che ogni problema introdotto da altri non si rifletta sulla reputazione degli autori originari.

Infine, ogni programma libero e' costantemente minacciato dai brevetti sui programmi. Vogliamo evitare il pericolo che chi ridistribuisce un Programma libero ottenga brevetti personali, rendendo percio' il Programma una cosa di sua proprieta'. Per prevenire questo, abbiamo chiarito che ogni prodotto brevettato debba essere distribuito per il libero uso da parte di chiunque, o non distribuito affatto.

Seguono i termini e le condizioni precisi per la copia, la distribuzione e la modifica.

LICENZA PUBBLICA GENERICA GNU TERMINI E CONDIZIONI PER LA COPIA, LA DISTRIBUZIONE E LA MODIFICA

0. Questa Licenza si applica a ogni Programma o altra opera che contenga una nota da parte del detentore del copyright che dica che tale opera puo' distribuita sotto i termini di questa Licenza Pubblica Generica. Il termine "Programma" nel seguito indica ognuno di questi programmi o lavori, e l'espressione "lavoro basato sul Programma" indica sia il Programma sia ogni opera considerata "derivata" in base alla legge sul Copyright: cioe' un lavoro contenente il programma o una porzione di esso, sia letteralmente sia modificato e/o tradotto in un'altra lingua; da qui in avanti, la traduzione e' in ogni caso considerata una "modifica". Vengono ora elencati i diritti dei detentori di licenza.

Attivita' diverse dalla copiatura, distribuzione e modifica non sono coperte da questa Licenza e sono al di fuori della sua influenza. L'atto di eseguire il programma non viene limitato, e l'output del programma e' coperto da questa Licenza solo se il suo contenuto costituisce un lavoro basato sul Programma (indipendentemente dal fatto che sia stato creato eseguendo il Programma). In base alla natura del Programma il suo output puo' essere o meno coperto da questa Licenza.

1. E' lecito copiare e distribuire copie letterali del codice sorgente del Programma cosi' come viene ricevuto, con qualsiasi mezzo, a condizione che venga riprodotta chiaramente su ogni copia una appropriata nota di copyright e di assenza di garanzia; che si mantengano intatti tutti i riferimenti a questa Licenza e all'assenza di ogni garanzia; che si dia a ogni altro destinatario del Programma una copia di questa Licenza insieme al Programma.

   E' possibile richiedere un pagamento per il trasferimento fisico di una copia del Programma, e' anche possibile a propria discrezione richiedere un pagamento in cambio di una copertura assicurativa.

2. E' lecito modificare la propria copia o copie del Programma, o parte di esso, creando percio' un lavoro basato sul Programma, e copiare o distribuire queste modifiche e questi lavori sotto i termini del precedente punto 1, a patto che anche tutte queste condizioni vengano soddisfatte:

   (a) Bisogna indicare chiaramente nei file che si tratta di copie modificate e la data di ogni modifica.

   (b) Bisogna fare in modo che ogni lavoro distribuito o pubblicato, che in parte o nella sua totalita' derivi dal Programma o da parti di esso, sia globalmente utilizzabile da terze parti secondo le condizioni di questa licenza.

(c) Se di solito il programma modificato legge comandi interattivamente quando eseguito, bisogna fare in modo che all'inizio dell'esecuzione interattiva usuale, stampi un messaggio contenente una appropriata nota di copyright e di assenza di garanzia (oppure che specifichi il tipo di garanzia che si offre). Il messaggio deve inoltre specificare agli utenti che possono ridistribuire il programma nelle condizioni qui descritte e deve indicare come reperire questa licenza. Se pero' il programma di partenza e' interattivo ma normalmente non stampa tale messaggio, non occorre che un lavoro derivato lo stampi.

Questi requisiti si applicano al lavoro modificato nel suo complesso. Se sussistono parti identificabili del lavoro modificato che non siano derivate dal Programma e che possono essere ragionevolmente considerate lavori indipendenti, allora questa Licenza e i suoi termini non si applicano a queste parti quando vengono distribuite separatamente. Se pero' queste parti vengono distribuite all'interno di un prodotto che e' un lavoro basato sul Programma, la distribuzione di questo prodotto nel suo complesso deve avvenire nei termini di questa Licenza, le cui norme nei confronti di altri utenti si estendono a tutto il prodotto, e quindi ad ogni sua parte, chiunque ne sia l'autore.

Sia chiaro che non e' nelle intenzioni di questa sezione accampare diritti su lavori scritti interamente da altri, l'intento e' piuttosto quello di esercitare il diritto di controllare la distribuzione di lavori derivati o dal Programma o contenenti esso.

Inoltre, se il Programma o un lavoro derivato da esso viene aggregato ad un altro lavoro non derivato dal Programma su di un mezzo di immagazzinamento o di distribuzione, il lavoro non derivato non deve essere coperto da questa licenza.

3. E' lecito copiare e distribuire il Programma (o un lavoro basato su di esso, come espresso al punto 2) sotto forma di codice oggetto o eseguibile sotto i termini dei precedenti punti 1 e 2, a patto che si applichi una delle seguenti condizioni:

   (a) Il Programma sia corredato dal codice sorgente completo, in una forma leggibile dal calcolatore e tale sorgente deve essere fornito secondo le regole dei precedenti punti 1 e 2 su di un mezzo comunemente usato per lo scambio di programmi.

   (b) Il Programma sia accompagnato da un'offerta scritta, valida per almeno tre anni, di fornire a chiunque ne faccia richiesta una copia

completa del codice sorgente, in una forma leggibile dal calcolatore, in cambio di un compenso non superiore al costo del trasferimento fisico di tale copia, che deve essere fornita secondo le regole dei precedenti punti 1 e 2 su di un mezzo comunemente usato per lo scambio di programmi.

(c) Il Programma sia accompagnato dalle informazioni che sono state ricevute riguardo alla possibilita' di avere il codice sorgente. Questa alternativa e' permessa solo in caso di distribuzioni non commerciali e solo se il programma e' stato ricevuto sotto forma di codice oggetto o eseguibile in accordo al precedente punto B. @end enumerate

Per "codice sorgente completo" di un lavoro si intende la forma preferenziale usata per modificare un lavoro. Per un programma eseguibile, "codice sorgente completo" significa tutto il codice sorgente di tutti i moduli in esso contenuti, piu' ogni file associato che definisca le interfacce esterne del programma, piu' gli script usati per controllare la compilazione e l'installazione dell'eseguibile. In ogni caso non e' necessario che il codice sorgente fornito includa nulla che sia normalmente distribuito (in forma sorgente o in formato binario) con i principali componenti del sistema operativo sotto cui viene eseguito il Programma (compilatore, kernel, e cosi' via), a meno che tali componenti accompagnino l'eseguibile.

Se la distribuzione dell'eseguibile o del codice oggetto e' effettuata indicando un luogo dal quale sia possibile copiarlo, permettere la copia del codice sorgente dallo stesso luogo e' considerata una valida forma di distribuzione del codice sorgente, anche se copiare il sorgente e' facoltativo per l'acquirente.

4. Non e' lecito copiare, modificare, sublicenziare, o distribuire il Programma in modi diversi da quelli espressamente previsti da questa Licenza. Ogni tentativo di copiare, modificare, sublicenziare o distribuire il Programma non e' autorizzato, e fara' terminare automaticamente i diritti garantiti da questa Licenza. D'altra parte ogni acquirente che abbia ricevuto copie, o diritti, coperti da questa Licenza da parte di persone che violano la Licenza come qui indicato non vedranno invalidare la loro Licenza, purche' si comportino conformemente ad essa.

5. L'acquirente non e' obbligato ad accettare questa Licenza, poiche' non l'ha firmata. D'altra parte nessun altro documento garantisce il permesso di modificare o distribuire il Programma o i lavori derivati da esso. Queste azioni sono proibite dalla legge per chi non accetta questa Licenza; percio', modificando o distribuendo il Programma o un lavoro

basato sul programma, si indica nel fare cio' l'accettazione di questa Licenza e quindi di tutti i suoi termini e le condizioni poste sulla copia, la distribuzione e la modifica del Programma o di lavori basati su di esso.

6. Ogni volta che il Programma o un lavoro basato su di esso vengono distribuiti, l'acquirente riceve automaticamente una licenza d'uso da parte del licenziatario originale. Tale licenza regola la copia, la distribuzione e la modifica del Programma secondo questi termini e queste condizioni. Non e' lecito imporre restrizioni ulteriori all'acquirente nel suo esercizio dei diritti qui garantiti. Chi distribuisce programmi coperti da questa Licenza non e' comunque responsabile per la conformita' alla Licenza da parte di terze parti.

7. Se, come conseguenza del giudizio di una corte, o di una imputazione per la violazione di un brevetto o per ogni altra ragione (anche non relativa a questioni di brevetti), vengono imposte condizioni che contraddicono le condizioni di questa licenza, che queste condizioni siano dettate dalla corte, da accordi tra le parti o altro, queste condizioni non esimono nessuno dall'osservazione di questa Licenza. Se non e' possibile distribuire un prodotto in un modo che soddisfi simultaneamente gli obblighi dettati da questa Licenza e altri obblighi pertinenti, il prodotto non puo' essere affatto distribuito. Per esempio, se un brevetto non permettesse a tutti quelli che lo ricevono di ridistribuire il Programma senza obbligare al pagamento di diritti, allora l'unico modo per soddisfare contemporaneamente il brevetto e questa Licenza e' di non distribuire affatto il Programma.

   Se parti di questo punto sono ritenute non valide o inapplicabili per qualsiasi circostanza, deve comunque essere applicata l'idea espressa da questo punto; in ogni altra circostanza invece deve essere applicato il punto 7 nel suo complesso.

   Non e' nello scopo di questo punto indurre gli utenti ad infrangere alcun brevetto ne' ogni altra rivendicazione di diritti di proprieta', ne' di contestare la validita' di alcuna di queste rivendicazioni; lo scopo di questo punto e' solo quello di proteggere l'integrita' del sistema di distribuzione dei programmi liberi, che viene realizzato tramite l'uso della licenza pubblica. Molte persone hanno contribuito generosamente alla vasta gamma di programmi distribuiti attraverso questo sistema, basandosi sull'applicazione fedele di tale sistema. L'autore/donatore puo' decidere di sua volonta' se preferisce distribuire il software avvalendosi di altri sistemi, e l'acquirente non puo' imporre la scelta del sistema di distribuzione.

Questo punto serve a rendere il piu' chiaro possibile cio' che crediamo sia una conseguenza del resto di questa Licenza.

8. Se in alcuni paesi la distribuzione e/o l'uso del Programma sono limitati da brevetto o dall'uso di interfacce coperte da copyright, il detentore del copyright originale che pone il Programma sotto questa Licenza puo' aggiungere limiti geografici espliciti alla distribuzione, per escludere questi paesi dalla distribuzione stessa, in modo che il programma possa essere distribuito solo nei paesi non esclusi da questa regola. In questo caso i limiti geografici sono inclusi in questa Licenza e ne fanno parte a tutti gli effetti.

9. All'occorrenza la Free Software Foundation puo' pubblicare revisioni o nuove versioni di questa Licenza Pubblica Generica. Tali nuove versioni saranno simili a questa nello spirito, ma potranno differire nei dettagli al fine di coprire nuovi problemi e nuove situazioni.

   Ad ogni versione viene dato un numero identificativo. Se il Programma asserisce di essere coperto da una particolare versione di questa Licenza e "da ogni versione successiva", l'acquirente puo' scegliere se seguire le condizioni della versione specificata o di una successiva. Se il Programma non specifica quale versione di questa Licenza deve applicarsi, l'acquirente puo' scegliere una qualsiasi versione tra quelle pubblicate dalla Free Software Foundation.

10. Se si desidera incorporare parti del Programma in altri programmi liberi le cui condizioni di distribuzione differiscano da queste, e' possibile scrivere all'autore del Programma per chiederne l'autorizzazione. Per il software il cui copyright e' detenuto dalla Free Software Foundation, si scriva alla Free Software Foundation; talvolta facciamo eccezioni alle regole di questa Licenza. La nostra decisione sara' guidata da due scopi: preservare la liberta' di tutti i prodotti derivati dal nostro free software e promuovere la condivisione e il riutilizzo del software in generale.

NON C'E' GARANZIA

11. POICHE' IL PROGRAMMA E' CONCESSO IN USO GRATUITAMENTE, NON C'E' GARANZIA PER IL PROGRAMMA, NEI LIMITI PERMESSI DALLE VIGENTI LEGGI. SE NON INDICATO DIVERSAMENTE PER ISCRITTO, IL DETENTORE DEL COPYRIGHT E LE ALTRE PARTI FORNISCONO IL PROGRAMMA "COSI' COM'E'", SENZA ALCUN TIPO DI GARANZIA, NE' ESPLICITA NE' IMPLICITA; CIO'

COMPRENDE, SENZA LIMITARSI A QUESTO, LA GARANZIA IMPLICITA DI COMMERCIABILITA' E UTILIZZABILITA' PER UN PARTICOLARE SCOPO. L'INTERO RISCHIO CONCERNENTE LA QUALITA' E LE PRESTAZIONI DEL PROGRAMMA E' DELL'ACQUIRENTE. SE IL PROGRAMMA DOVESSE RIVELARSI DIFETTOSO, L'ACQUIRENTE SI ASSUME IL COSTO DI OGNI MANUTENZIONE, RIPARAZIONE O CORREZIONE NECESSARIA.

12. NE' IL DETENTORE DEL COPYRIGHT NE' ALTRE PARTI CHE POSSONO MODIFICARE O RIDISTRIBUIRE IL PROGRAMMA COME PERMESSO IN QUESTA LICENZA SONO RESPONSABILI PER DANNI NEI CONFRONTI DELL'ACQUIRENTE, A MENO CHE QUESTO NON SIA RICHIESTO DALLE LEGGI VIGENTI O APPAIA IN UN ACCORDO SCRITTO. SONO INCLUSI DANNI GENERICI, SPECIALI O INCIDENTALI, COME PURE I DANNI CHE CONSEGUONO DALL'USO O DALL'IMPOSSIBILITA' DI USARE IL PROGRAMMA; CIO' COMPRENDE, SENZA LIMITARSI A QUESTO, LA PERDITA DI DATI, LA CORRUZIONE DEI DATI, LE PERDITE SOSTENUTE DALL'ACQUIRENTE O DA TERZE PARTI E L'INABILITA' DEL PROGRAMMA A LAVORARE INSIEME AD ALTRI PROGRAMMI, ANCHE SE IL DETENTORE O ALTRE PARTI SONO STATE AVVISATE DELLA POSSIBILITA' DI QUESTI DANNI.

FINE DEI TERMINI E DELLE CONDIZIONI

Appendice: come applicare questi termini ai nuovi programmi

Se si sviluppa un nuovo programma e lo si vuole rendere della maggiore utilita' possibile per il pubblico, la cosa migliore da fare e' rendere tale programma free software, cosicche' ciascuno possa ridistribuirlo e modificarlo sotto questi termini.

Per fare questo, si inserisca nel programma la seguente nota. La cosa migliore da fare e' mettere la nota all'inizio di ogni file sorgente, per chiarire nel modo piu' efficiente possibile l'assenza di garanzia; ogni file dovrebbe contenere almeno la nota di copyright e l'indicazione di dove trovare l'intera nota.

‹una riga per dire in breve il nome del programma e cosa fa›
Copyright (C) 19aa
‹nome dell'autore›

Questo programma e' free software; e' lecito redistribuirlo e/o modificarlo secondo i termini della Licenza Pubblica Generica GNU come e' pubblicata dalla Free Software Foundation; o la versione 2 della licenza o (a propria scelta) una versione successiva.

Questo programma e' distribuito nella speranza che sia utile, ma SENZA ALCUNA GARANZIA; senza neppure la garanzia implicita di NEGOZIABILITA' o di APPLICABILITA' PER UN PARTICOLARE SCOPO. Si veda la Licenza Pubblica Generica GNU per avere maggiori dettagli.

Ognuno dovrebbe avere ricevuto una copia della Licenza Pubblica Generica GNU insieme a questo programma; in caso contrario, si scriva alla Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, Stati Uniti. Si aggiungano anche informazioni su come si puo' essere contattati tramite posta elettronica e cartacea.

Se il programma e' interattivo, si faccia in modo che stampi una breve nota simile a questa quando viene usato interattivamente:

Orcaloca versione 69, Copyright (C) 19aa <nome dell'autore> Orcaloca non ha ALCUNA GARANZIA; per i dettagli si digiti 'show g'. Questo e' free software, e ognuno e' libero di ridistribuirlo sotto certe condizioni; si digiti 'show c' per dettagli.
Gli ipotetici comandi "show g" e "show c" mostreranno le parti appropriate della Licenza Pubblica Generica. Chiaramente, i comandi usati possono essere chiamati diversamente da "show g" e "show c" e possono anche essere selezionati con il mouse o attraverso un menu'; in qualunque modo pertinente al programma.

Se necessario, si dovrebbe anche far firmare al proprio datore di lavoro (se si lavora come programmatore) o alla propria scuola, se si e' studente, una "rinuncia al copyright" per il programma. Ecco un esempio con nomi fittizi:

Yoyodinamica SPA rinuncia con questo documento ad ogni interesse al copyright del programma 'Orcaloca' (che svolge dei passi di compilazione) scritto da Giovanni Smanettone.

‹firma di Primo Tizio›, 1 April 1999 Primo Tizio, Presidente

I programmi coperti da questa Licenza Pubblica Generica non possono essere incorporati all'interno di programmi proprietari. Se il proprio programma e' una libreria di funzioni, puo' essere piu' utile permettere di collegare applicazioni proprietarie alla libreria. Se si ha questa intenzione consigliamo di usare la Licenza Generica Pubblica GNU per Librerie (LGPL) al posto di questa Licenza.

Bibliografia

[Alm96] ALMESBERGER, Werner: *LILO User's guide*, 1996. – (siehe Datei `/usr/share/doc/lilo/user.dvi`)

[Bai97] BAILEY, Edward C.: *Maximum RPM*. Red Hat, 1997. – (ISBN 1-888172-78-9)

[BBD+97] BECK, Michael; BÖHME, Harald; DZIADZKA, Mirko; KUNITZ, Ulrich; MAGNUS, Robert ; VERWORNER, Dirk: *Linux-Kernel-Programmierung*. 4. Aufl. Addison Wesley GmbH, 1997. – (ISBN 3-8273-1144-6)

[BD98] BORKNER-DELCARLO, Olaf: *Linux im kommerziellen Einsatz*. Carl Hanser Verlag, 1998. – (ISBN 3-446-19465-7)

[BD99] BORKNER-DELCARLO, Olaf: *Das Samba-Buch*. SuSE PRESS, 1999. – (ISBN 3-930419-93-9)

[CAR93] COSTALES, Bryan; ALLMAN, Eric ; RICKERT, Neil: *sendmail*. O'Reilly & Associates, Inc., 1993. – (ISBN 1-56592-056-2)

[CB96] CHESWICK, William R.; BELLOVIN, Steven M.: *Firewalls und Sicherheit im Internet*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-875-x)

[CZ96] CHAPMAN, Brent; ZWICKY, Elisabeth D.: *Einrichten von Internet Firewalls. Sicherheit im Internet gewährleisten.*. O'Reilly & Associates, Inc., 1996. – (ISBN 3-930673312)

[DR99] DAWSON, Terry; RUBINI, Alessandro: *NET3-4 HOWTO*, v1.5, August 1999. – (siehe Datei `/usr/share/doc/howto/en/NET3-4-HOWTO.gz`)

[EH98] ECKEL, George; HARE, Chris: *Linux – Internet Server*. Carl Hanser Verlag, 1998. – (ISBN 3-446-19044-9)

[FCR93] FANG, Chin; CROSSON, Bob ; RAYMOND, Eric S.: *The Hitchhiker's Guide to X386/XFree86 Video Timing (or, Tweaking your Monitor for Fun and Profit)*, 1993. – (siehe Datei `/usr/X11/lib/X11/doc/VideoModes.doc`)

[Fis00] FISCHER, Thorsten: *GUI-Programmierung mit GTK+ (Handbuch und Referenz)*. SuSE PRESS, 2000. – ISBN (3–934678–42–4)

[Fri93] FRISCH, Æleen: *Essential System Administration*. O'Reilly & Associates, Inc., 1993. – (ISBN 0-937175-80-3)

[Gil92] GILLY, Daniel: *UNIX in a nutshell: System V Edition*. O'Reilly & Associates, Inc., 1992. – (ISBN 1-56592-001-5)

[GMR97] GOOSSENS, Michel; MITTELBACH, Frank ; RAHTZ, Sebastian: *The LaTeX Graphics Companion*. Addison Wesley Longman, 1997. – (ISBN 0-201-85469-4)

[GMS94] GOOSSENS, Michel; MITTELBACH, Frank ; SAMARIN, Alexander: *The LaTeX Companion*. Addison Wesley GmbH, 1994. – (ISBN 0-201-54199-8)

[GMS96] GOOSSENS, Michel; MITTELBACH, Frank ; SAMARIN, Alexander: *Der LaTeX-Begleiter*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-646-3)

[GR99] GOOSSENS, Michel; RAHTZ, Sebastian: *The LaTeX Web Companion*. Addison Wesley Longman, 1999. – (ISBN 0-201-43322-7)

[GS93] GARFINKEL, Simson; SPAFFORD, Gene: *Practical UNIX Security*. O'Reilly & Associates, Inc., 1993. – (ISBN 0-937175-72-2)

[Hei96] HEIN, Jochen: *Linux-Companion zur Systemadministration*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-869-5)

[Her92] HEROLD, H.: *UNIX Grundlagen*. Addison Wesley GmbH, 1992. – (ISBN 3-89319-542-8)

[HHMK96] HETZE, Sebastian; HOHNDEL, Dirk; MÜLLER, Martin ; KIRCH, Olaf: *Linux Anwenderhandbuch*. 6. Aufl. LunetIX Softfair, 1996. – (ISBN 3-929764-05-9)

[Hof97] HOFFMANN, Erwin: EMail-Gateway mit qmail. In: *iX* 12 (1997), S. 108ff.

[HR98] HÖLZER, Matthias; RÖHRIG, Bernhard: *KDE – Das K Desktop Environment*. Computer & Literatur, 1998. – (ISBN 3-932311-50-7)

[Hun95] HUNT, Craig: *TCP/IP Netzwerk Administration*. O'Reilly & Associates, Inc., 1995. – (ISBN 3-930673-02-9)

[JT98] JOHNSON, Michael K.; TROAN, Erik W.: *Anwendungen entwickeln unter Linux*. Addison Wesley GmbH, 1998. – (ISBN 3-8273-1449-6)

[Kie95] KIENLE, Micheal: TIS: Toolkit für anwendungsorientierte Firewall-Systeme. In: *iX* 8 (1995), S. 140ff.

[Kir95] KIRCH, Olaf: *LINUX Network Administrator's Guide*. O'Reilly & Associates, Inc., 1995. – (ISBN 1-56592-087-2)

[Kof99] KOFLER, Michael: *Linux – Installation, Konfiguration, Anwendung*. 4. Aufl. Addison Wesley GmbH, 1999. – (ISBN 3-8273-1475-5)

[Kop94] KOPKA, Helmut: *LaTeX-Einführung*. Addison Wesley GmbH, 1994. – (ISBN 3-89319-664-1)

[Kopff] KOPKA, Helmut: *LaTeX*. Addison Wesley GmbH, 1996 ff. – 3 Bde. (ISBN 3-8273-1025-3; 3-8273-1229-9; 3-89319-666-8)

[Kun95] KUNITZ, Ulrich: Sicherheit fast kostenlos: Einrichtung eines kostenlosen Firewall-Systems. In: *iX* 9 (1995), S. 176ff.

[Lam90] LAMB, Linda: *Learning the vi Editor*. O'Reilly & Associates, Inc., 1990. – (ISBN 0-937175-67-6)

[Lef96] LEFFLER, Sam: *HylaFAX Home Page*, 1996

[Meg98] MEGGINSON, David: *Structuring XML Documents*. Prentice-Hall, 1998. – ISBN (0–13–642299–3)

[Moh98] MOHR, James: *UNIX-Windows-Integration*. International Thomson Publishing, 1998. – (ISBN 3-8266-4032-2)

[OT92] O'REILLY, Tim; TODINO, Grace: *Managing UUCP and Usenet*. O'Reilly & Associates, Inc., 1992. – (ISBN 0-937175-93-5)

[POL97] PEEK, Jerry; O'REILLY, Tim ; LOUKIDES, Mike: *Unix Power Tools*. 2. Aufl. Sebastopol : O'Reilly & Associates, Inc., 1997

[Rub98] RUBINI, Alessandro: *Linux-Gerätetreiber*. O'Reilly & Associates, Inc., 1998. – (ISBN 3-89721-122-X)

[Sch98] SCHEIDERER, Jürgen: Sicherheit Kostenlos - Firewall mit Linux. In: *iX* 12 (1998)

[Sto98] STOLL, Clifford: *Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten*. Fischer-TB.-Vlg., 1998. – (ISBN 3596139848)

[SuS02a] *SuSE Linux. Basis*. 1. Nürnberg : SuSE Linux AG, 2002

[SuS02b] *SuSE Linux. Benutzerhandbuch*. 1. Nürnberg : SuSE Linux AG, 2002

[SuS02c] *SuSE Linux. Die Programme*. 1. Nürnberg : SuSE Linux AG, 2002

[The96] THE XFREE86™-TEAM: *XF86Config(4/5) – Configuration File for Xfree86™*, 1996. – Manual-Page zu XFree86™

[TSP93] TODINO, Grace; STRANG, John ; PEEK, Jerry: *Learning the UNIX operating system*. O'Reilly & Associates, Inc., 1993. – (ISBN 1-56592-060-0)

[Tun99] TUNG, Brian: *Kerberos: A Network Authentication System*. Fischer-TB.-Vlg., 1999. – (ISBN 0-201-37924-4)

[Wel94] WELSH, Matt: *Linux Installation and Getting Started*. 2. Aulf. SuSE GmbH, 1994. – (ISBN 3-930419-03-3)

[WK95] WELSH, Matt; KAUFMAN, Lars: *Running Linux*. O'Reilly & Associates, Inc., 1995. – (ISBN 1-56592-100-3)

[WK98] WELSH, Matt; KAUFMAN, Lars: *Linux – Wegweiser zur Installation & Konfiguration*. 2. Aufl. O'Reilly & Associates, Inc., 1998. – (ISBN 3-930673-58-4)

[WM99] WALSH, Norman; MUELLNER, Leonard: *DocBook. The Definiteve Guide*. O'Reilly & Associates, Inc., 1999. – ISBN (1–56592–580–7)

Indice analitico

Simboli

`/etc/conf.modules` 139
/etc/hosts 195
`/etc/inittab` 160
`/etc/modules.conf` 139
/etc/named.conf 232
`/etc/profile` ..... *vedi* bash, /etc/profile
`/etc/resolv.conf` 147
xdm 178

A

Advanced Powermanagement 190
AMaViS 170
Amministrazione utenti ..... *vedi* YaST2, amministrazione utenti
Apache
- Squid 286
Apple
- Netatalk 263
apsfilter
- stampante rete 121
`autoexec.bat` 165
autofs 174

B

bash
- `/etc/profile` 143
BIND 230
Boot 159, 327
- Concetto di 159
Box di server di stampante 121

C

Check 327
Client NFS 245
Collegamenti in rete 203
Comando
- `ulimit` 146
command not found 195
Compose ..... *vedi* Mappatura della tastiera, Compose
`conf.modules` 139
Configurare
- Fuso orario 30
- Reti
  · Manualmente 229
- YaST2 9
Configurazione
- Impostare lorario con NTP 198
- IPv6 220
- manuale 221
- Modificare 167
- Reti
  · Manualmente 221
- Squid 278
Configurazione del sistema 169
Configurazione dello schermo 15
Console 175
- virtuali 148
console di testo 178
Console virtuali 148
Core-file 146
Crash 327
cron 144, 176

D

DCF77 198
Demone Syslog
- configurare 196
- syslog-ng 196
depmod 138
DHCP

- Configurazione del client 186
- Configurazione server 178
- Relay agent 178
Diritti 193
- Diritti dei file 145
Diritti sui file 193
DMA
- Attivare 179
- Disattivare 179
DNS 211, 230
- File zona 235
- Forwarding 231
- Logging 234
- Mail Exchanger 212
- NIC 211
- Opzioni 233
- server 18
- Squid e 277
- top level domain 211
- Zone 234
DNS:Risoluzione inversa dellindirizzo .. 238
Domain Name Service ..... *vedi* NIS
Dominio DNS 243
Dominio NIS 243
DVB 179

E

E-mail
- Configurare con YaST2 17
e2fsck
- Manual-Page 327
esportare 246

F

FHS ..... *vedi* Filesystem, FHS
file di configurazione 169
File di configurazione 221
- dhcp 222
- export 247
- Host 222
- host.conf 223
- HOSTNAME 227
- nscd.conf 225
- nsswitch.conf 224
- rc.config 26
- resolv.conf 226
- Rete 222
- routes 228
- routing 228
- squid.conf 278, 283, 286
- squidguard.conf 288
- SuSEfirewall2 295–297
- wireless 222
- XF86Config 35
File di log 144
- boot.msg 30
- Comunicazioni 297
- Messaggi 30
- XFree86.0.log 35
File system
- Intermezzo 181
File temporanei
- Cancellare 176
- Cancellare al boot 177
Filesystem
- FHS 142
- TeX 142
Firewall 22, 292–295, 297
- Attivare 170
- Filtri di pacchetti 294
- Filtro di pacchetti 292
- Squid e 284
- SuSEfirewall2 ..... 292, 295–297
· Configurare 297
· Configurazione 295
Frame buffer 175
`free` 147
Fuso orario 175

G

Ghostscript 107
GPL 333
Graphica
- 3D 170
group 243
Gruppi
- Amministrazione in YaST2 20
gs ..... *vedi* Ghostscript

H

hardware ..... *vedi* YaST2,informazione hardware
Hardware
- Hotplug 179
- Joystick 182
- Stampante 193
httpd 170

I

I18N 149
Identifier 47
importare 245
Impostazioni di sicurezza 20
Impostazioni X11 15
Indirizzi
- IP 207

- MAC 208
Indirizzi IP 207
- Classi di rete 208
- IPv6
· Configurare 220
· Configurazione 214
· Maschere di rete 216
· Prefissi 215
- Maschere di rete 208
- Masquerading 292–294
- privati 210
Indirizzo IP
- dinamico 195
Indirizzo IP dinamico 195
Info (`info`) 146
Inidirizzi IP
- IPv6 212
init 160
- Script 163
initrd 182
inittab 160
insmod 138
Installare la stampante 15
Installare/rimuovere software ..... *vedi* YaST2,software
Installazione
- Autoinstallazione 174
Interfaccia
- IrDA 75
- seriale 76
- USB 73
Interfaccia grafica 15
Intermezzo 181
IP-Forwarding 196
IrDA
- Impostare linterfaccia 181
iso-8859 50
ispell 181
ITNIC 230

J

Java 181

K

KDM
- Comportamento di spegnimento . 21
kernel 137
- moduli 138
Kernel
- Debugging 196
- Sysrq 196
Konsole 178

L

L10N 149
Lan
- Configurare 218
LAN
- Configurare 229
Licenza 333
Linux Standard Base 142
Local Area Network ..... *vedi* LAN
locate 184
Logical Volume Manager
- YaST2 27
Login 178
Lorario del sistema 174
lpc 78
lpd 77
lpq 78
lpr 78
lprm 78
LSB ..... *vedi* Linux Standard Base
lsmod 139

M

Mac OS 263
Mail
- Postfix 179
Mappatura della tastiera 148
- Compose 148
Masquerading 292–294
- Configurare con SuSEfirewall2 .. 295
- Difficoltà 294
- IP-Forwarding 196
- ipchains 293
- iptables 293
Maus 185
Memoria
- RAM 147
Mezzo di installazione . *vedi* YaST2, mezzo di installazione
Modeline 48
modprobe 138
`modules.conf` 139
moduli 138
Moduli del kernel
- Scheda di rete 218
Modulo
- uso 138
mount 246
mountd 246
Multi_key .... *vedi* Mappatura della tastiera, Compose
Multihead 40

N

Name Service Cache Daemon 225
Name Service Switch 224
NAT ..... *vedi* masquerading
Netatalk 263
NetBIOS 256
Network File System ..... *vedi* NFS
Network Information Service ..... *vedi* NIS
NFS 245
- Server 17
nfsd 246
NIS 240
- Client 243
NNTP-Server 189
Notebook
- PCMCIA 189
NSS
- banche dati 224

O

Online-Update ... *vedi* YaST2,Online-Update
OpenSSH ..... *vedi* SSH
Orologio radiotelecomandato 198

P

pacchetto
- `3dpixms` 197
- `a2ps` 111
- `aaa_base` 144
- `bind8` 239
- `binutils` 137
- `cross-ppc64-gcc` 137
- `cups` 98, 103
- `cups-client` 63, 69, 103
- `cups-drivers` 68, 98
- `cups-drivers-stp` 68, 98, 101
- `cups-libs` 63
- `dhcpcd` 251
- `exports` 246
- `fhs` 142
- `findutils-locate` 177
- `ftpdir` 142
- `gcc` 137
- `glibc-devel` 137
- `glibc-info` 152
- `gv` 108, 118
- `howtoen` 290, 294
- `isapnp` 72
- `kernel-source` 137
- `libcinfo` 224
- `logrotate` 144, 194
- `lpdfilter` 83
- `lprng` 63, 77, 122, 123
- `named` 224
- `netatalk` 263, 269
- `openssh` 298
- `psutils` 85, 113
- `radvd` 220
- `samba` 257
- `samba-client` 99, 101, 124
- `squidgrd` 288
- `SuSEfirewall2` 170, 292
- `ttmkfdir` 51
- `xntp` 198
- `yudit` 51

Pagine di manuale ..... 146, *vedi* Pagine di manuale
- Creare database 177
Pagine gialle ..... *vedi* NIS
Partizioni
- YaST2 e 27
passwd 243
Patch-CD-Update ..... *vedi* YaST2,Patch-CD-Update
PCMCIA 189
Permessi
- default 22
Permissions 193
Porta
- parallela 70
Porte
- Scansionare 285
portmap 246
Portmapper RPC 245, 246
Postfix
- Mail Relaying 179
Print-Manager (lpd) 77
profondità dei colori 46
Programmare
- Core-file 146
Protocolli
- ICMP 205
- IGMP 205
- TCP/IP 204
- UDP 205
Proxy
- FTP 193
- HTTP 193
- Squid 272
- Trasparente 283
- Vantaggi 272

R

Ramdisk
- Initial Ramdisk 182
Reboot 178

resolv.conf ..... *vedi* /etc/resolv.conf
Rete 16
- Autenticazione
· Kerberos 303
- Configurare il server DHCP 178
- Configurare la sceda di rete 188
- Configurazione
· IPv6 220
- Configurazione di base 185
- DHCP relay 178
- DNS 211
- E-Mail 184
- File di configurazione 221, 227
- Indirizzi IP 207
- Indirizzo broadcast 210
- Indirizzo di base della rete 210
- Localhost 210
- NFS 189
- Routing 207, 208
- software di monitor 173
- YaST2 e 16
- Zope 199
Reti 203
- Configurare 218, 229
- Integrare 218–229
- Maschere di rete 208
Risoluzione dello schermo 46
rmmod 138
Router
- IP-Forwarding 196
Routing 207, 228, 229
- Maschere di rete 208
- Masquerading 292–294
- routes 228
- statico 228
RPC-mount-daemon 246
RPC-NFS-daemon 246
RPM
- Database 174
Runlevel 160
- Editare in YaST2 26
- Passaggio di 162
Runlevel Editor 166

S

Samba 256
- Security Level 260
SaX2
- Multihead 40
Scheda di rete 16
Scheda grafica 15
Schede
- Reti
· Testare 218
Schede PC 189
Schermo virtuale 46
Script
- init.d
· inetd 227
· network 227
· nfsserver 228
· portmap 228
· sendmail 228
· ypbind 228
· ypserv 228
- init.d/squid 276
- modify_resolvconf 226
Script startup
- init.d 227
secure shell 297
Secure Shell Daemon 194
Security Level
- Samba 260
serie
- `doc` 152, 224
- `n` 220, 257, 290
- `xap` 51
Server dei nomi 230
- BIND 230
Server di stampante 121
Server FTP
- configurare 142
Server HTTP
- impostare 143
Server NFS 245
Server NIS 243
servizio del nome 256
Share 257
Shutdown 178
Sicurezza 292–297
- Firewall 292–297
- Squid 272
- SSH 297
- SSH) 303
Sicurezza del sistema . *vedi* YaST2,Sicurezza del sistema
Sistema
- Lingua 30
Sistema spool
- Controllo 78
- Demone 77
- Stampante rete 121
SMB 256
Soft-RAID ..... *vedi* YaST2,Soft-RAID
Squid 272
- Apache 286

- Avviare 276
- Cache 273
- cachemgr.cgi 286
- Calamaris 289
- Configurazione 278
- Controllo dellaccesso 280, 286
- CPU 276
- Dimensioni della cache 275
- Directory 276
- Diritti 280
- Disco rigido 275
- Disinstallare 277
- DNS 277
- File di log 277
- Firewall 284
- Memorizzare oggetti 274
- Proprietà 272
- Proxy trasparente 283
- Proxy-Cache 272
- RAM 275
- SARG 290
- Sicurezza 272
- SquidGuard 287
- Statistiche 286

SSH 297–303
- Autenticazione 301
- scp 299
- sftp 299
- ssh-agent 302
- sshd 300

Stampa, sistema di ..... *vedi* Spool-System
Stampante
- Demone 77

Stampante di rete 121
Stampante rete
- Prefiltraggio 121

Stampante, filtro della
- Per stampanti rete 121

Stampare 15, 53
- Eliminare disfunzioni 82
- Linguaggio della stampante 54
- Stampante GDI 59

SuSEconfig 194
SuSEconfig 167
SuSEConfig 167
SuSE Linux Enterprise Server
- Mappatura della tastiera 148

Syn Flood Protection 195
`/etc/sysconfig` 167
Sysrq ..... *vedi* Kernel, Sysrq

T

Tastiera
- CapsLock 183
- Layout 183
- NumLock 183
- Ripetizione 183
- ScrLock 183
- Velocità di reazione 183

TCP/IP 204
- ICMP 205
- IGMP 205
- Modelli a strati 205
- pacchetti 205
- Pacchetto 207
- Servizi 204
- TCP 204
- UDP 205

Terminali X 197
TeX 196
Texinfo 146
Tkinfo (`tkinfo`) 146
True Type ..... *vedi* X11, True Type

U

UDP ..... *vedi* TCP
ugidd 248
`ulimit` 146
Unicode 50

V

Variabile d'ambiente
- `LANG` 183
- `LC_*` 183
- `PATH` iv
- `PRINTER` 78

W

whois 212
Window manager 197
Windows 256
- SMB 256

X

X 33
- Storia 33
- XFree86 33

X Window System ..... *vedi* X
X11
- Display manager 178
- driver 47
- Font 49
- Font TrueType 49
- mkfontdir 49
- ottimizzare 43
- set di caratteri 49

- ttmkfdir 49
XF86Config
- Clocks 46
- Depth 46
- Device 44, 46, 47
- Files 44
- InputDevice 44
- modeline 46
- Modeline 44
- Modes 44, 46, 48
- Monitor 44, 46, 48
- Screen 45
- ServerFlags 44
- ServerLayout 45
- Subsection
· Display 46
- Virtual 47
XInfo (`xinfo`) 146

Y

YaST
- mappatura della tastiera 3
- modo testo 3
- ncurses 3
YaST2
- Aggiornamento in linea tramite console 11
- Amministrazione degli utenti 19
- Amministrazione gruppi 20
- backup 24
- CD dei driver del produttore 31
- Configurare il sistema 9
- Configurazione della rete ... 218–220
- Configurazione dello schermo ... 15
- Disinstallazione software 12
- Editor dei runlevel 26
- Editor per sysconfig 26
- Editor Sysconfig 168
- firewall 22
- Fuso orario 30
- Hardware 15
- Informazione hardware 16
- Installare la stampante 15
- Installazione software 12
- interfaccia grafica 15
- Lingua 30
- Logical Volume Manager 27
- LVM 27
- Mezzo di installazione 11
- Partizionatore 27
- Patch-CD-Update 15
- postfix 17
- rc.config 26, 168
- Rete 16
- Routing 19
- Runlevel Editor 166
- scheda grafica 15
- sendmail 17
- Server DNS 18
- Server NFS 17
- Server NIS 18
- Sicurezza del sistema 20
- Soft-RAID 28
- Stampare 15
- update 14
- YaST Online Update 11
- Yellow Pages .... *vedi* YaST2, Server NIS
- YOU 11, 189
YOU ..... *vedi* YaST2,YOU
YP
- Opzioni 199
yudit 50

Z

Zope 199